

ON AUTOMORPHISMS OF BIPRODUCTS

DAVID E. RADFORD

ABSTRACT. We study certain subgroups of the full group of Hopf algebra automorphisms of a biproduct. In the process interesting subgroups of certain permutation groups come into play.

INTRODUCTION

Biproducts account for many examples of semisimple Hopf algebras over a field k . In [9] we studied a class of Hopf biproducts $A = B \times H$, where $B = k[\mathcal{G}]$ and $H = k[G]$ are group algebras, and described their coalgebra structures in detail. These biproducts are those of Theorem 7. In important special cases we were able to describe the algebra structure of A in detail as well. A followup to [9] is the study Hopf algebra automorphisms of A .

Let A, H be any Hopf algebras over k and suppose $A = B \times H$ is a biproduct. The biproduct structure of A is determined by Hopf algebra maps $\pi : A \rightarrow H$ and $j : H \rightarrow A$ which satisfy $\pi \circ j = \text{Id}_H$. In this paper we will also think of biproducts as quadruples (A, H, π, j) , where A, H are Hopf algebras over k and π, j are Hopf algebra maps as just described. A notion of automorphism of the biproduct (A, H, π, j) is a Hopf algebra automorphism F of A which satisfies $\pi \circ F = \pi$ and $F \circ j = j$. These form a subgroup $\text{Aut}_{\text{Hopf}}(A, \pi, j)$ of the group of Hopf algebra automorphisms $\text{Aut}_{\text{Hopf}}(A)$ of A under function composition.

Now B is a Hopf algebra in the Yetter-Drinfel'd category ${}^H_H\mathcal{YD}$. We show that $\text{Aut}_{\text{Hopf}}(A, \pi, j) \simeq \text{Aut}_{\mathcal{YD}-\text{Hopf}}(B)$, the group of Hopf algebra automorphisms in the category ${}^H_H\mathcal{YD}$ in Theorem 2. Thus we find the two conditions $\pi \circ F = \pi$ and $F \circ j = j$ too restrictive. We relax the second.

The set $\text{Aut}_{\text{Hopf}}(A, \pi)$ of Hopf algebra automorphisms F of A satisfying $\pi \circ F = \pi$ is a subgroup of $\text{Aut}_{\text{Hopf}}(A)$. The study of $\text{Aut}_{\text{Hopf}}(A, \pi)$ is the focus of this paper.

Let $F \in \text{Aut}_{\text{Hopf}}(A, \pi)$. Then we define two maps $F_L : B \rightarrow B$ and $F_R : H \rightarrow B$ which provide a “factorization” of F . It is always the case that F_L is an algebra automorphism of B and $\nu : \text{Aut}_{\text{Hopf}}(A, \pi) \rightarrow \text{Aut}_{\text{Alg}}(B)$ defined by $\nu(F) = F_L$ is a group homomorphism.

Whether or not $F_L \in \text{Aut}_{\mathcal{YD}-\text{Hopf}}(B)$ is a major theme of this paper. If $\text{Im}(\nu) \subseteq \text{Aut}_{\mathcal{YD}-\text{Hopf}}(B)$ then

$$(0.1) \quad \text{Aut}_{\text{Hopf}}(A, \pi) \simeq \text{Aut}_{\mathcal{YD}-\text{Hopf}}(B) \times \mathcal{N}(B, H)$$

as groups, where the right hand side has a semidirect product structure and $\mathcal{N}(B, H) \simeq \text{Ker}(\nu)$. See Corollary 6.

Whether or not $F_L \in \text{Aut}_{\mathcal{Y}\mathcal{D}_{\text{Hopf}}}(B)$ comes down to whether or not F_L is map of left H -modules and a map of coalgebras. Suppose that B is commutative as a k -algebra and H is cocommutative. Then F_L is a module map. Hence in this case $F_L \in \text{Aut}_{\mathcal{Y}\mathcal{D}_{\text{Hopf}}}(B)$ if and only if F_L is a coalgebra map. Whether or not F_L is a coalgebra map is a fascinating and involved problem to investigate.

We are most interested in the biproducts $A = k[\mathcal{G}] \times k[G]$ of Theorem 7 when \mathcal{G} and G are finite groups, \mathcal{G} abelian. Some minor restrictions need to be placed on the field k . We show that whether or not the decomposition of $\text{Aut}_{\text{Hopf}}(A, \pi)$ described in (0.1) holds boils down to the nature of a certain subgroup $\Gamma(\mathbf{G}, \lambda, \sigma)$, where \mathbf{G} is the additive version of \mathcal{G} , of the group of permutations $\text{Sym}(\mathbf{G})$ of the set \mathbf{G} under function composition. See Section 9, Theorems 7 and 11. We use the standard notations \leq and $<$ for “is a subgroup of” and “is a proper subgroup of” respectively.

The group $\Gamma(\mathbf{G}, \lambda, \sigma)$ is described in terms of certain elements of the character group \widehat{G} . This group should be of interest in its own right as well as a generalization studied in Sections 11 and 13.

Throughout k is a field and all vector spaces are over k , though we use the redundant expression “over k ” quite often. The group of units of k is denoted k^\times . For vector spaces U and V we drop the subscript k from $\text{Hom}_k(U, V)$, $\text{End}_k(U)$, and $U \otimes_k V$. If W is subspace of U and $f : U \rightarrow V$ is a map of vector spaces then $f|_W : W \rightarrow V$ denotes the restriction of f to W .

Let A be an algebra. Then $Z(A)$ denotes the center of A and 1 or 1_A denotes the multiplicative neutral element of A . Minor exception, Id_U denotes the identity map of a vector space U .

Let C be a coalgebra. We use a shorthand version of the Heyneman-Sweedler notation for expressing the coproduct in writing $\Delta(c) = c_{(1)} \otimes c_{(2)}$ for $c \in C$. For a coalgebra C and an algebra D over k we let “ \star ” denote the convolution product of $\text{Hom}(C, D)$. We suggest any of [1, 3, 5, 8, 10, 14] as a Hopf algebra reference. Good general algebra references are [4, 13].

1. PRELIMINARIES

Let H be a Hopf algebra over the field k . Then a biproduct of the form $A = B \times H$ is the tensor product $B \otimes H$ as a vector space. The vector space B is an algebra, coalgebra, left H -module, and a left H -comodule over k . There are natural compatibilities among these structures which we will list for the reader’s convenience. As an algebra $A = B \# H$ is a smash product and as a coalgebra $A = B \sharp H$ is a smash coproduct. The compatibilities are expressed by B is a left H -module algebra and coalgebra, by B is a left H -comodule algebra and coalgebra, and by connections between the algebra and coalgebra structures of B and the module and comodule structures

on B . If C is a coalgebra and (M, ρ) is a left C -comodule then we write $\rho(m) = m_{(-1)} \otimes m_{(0)} \in C \otimes M$ for all $m \in M$.

A left H -module algebra is a left H -module (B, \cdot) , where B is an algebra over k , such that $h \cdot 1 = \epsilon(h)1$ and $h \cdot (bb') = (h_{(1)} \cdot b)(h_{(2)} \cdot b')$ for all $h \in H$ and $b, b' \in B$. If (B, \cdot) is a left H -module algebra the tensor product $B \otimes H$ of vector spaces has an algebra structure, referred to as the smash product, defined by $1_{B \otimes H} = 1_B \otimes 1_H$ and

$$(1.1) \quad (b \otimes h)(b' \otimes h') = b(h_{(1)} \cdot b') \otimes h_{(2)} h'$$

for all $b, b' \in B$ and $h, h' \in H$. Typical notation for this algebra is $B \# H$ and tensors $b \otimes h$ are written $b \# h$. Observe $(b \# h)(b' \# h') = bb' \# hh'$ if either $h = 1$ or $b' = 1$. As a consequence the maps $H \longrightarrow B \# H$ and $B \longrightarrow B \# H$ defined by $h \mapsto 1 \# h$ and $b \mapsto b \# 1$ respectively are a one-one algebra maps.

A left H -comodule algebra is a left H -comodule (B, ρ) , where B is an algebra over k , such that $\rho(1) = 1_H \otimes 1$ and $\rho(bb') = b_{(-1)} b'_{(-1)} \otimes b_{(0)} b'_{(0)}$ for all $b, b' \in B$. A left H -module coalgebra is a left H -module (C, \cdot) , where C is a coalgebra over k , such that $\epsilon(h \cdot c) = \epsilon(h)\epsilon(c)$ and $\Delta(h \cdot c) = h_{(1)} \cdot c_{(1)} \otimes h_{(2)} \cdot c_{(2)}$ for all $h \in H$ and $c \in C$.

A left H -comodule coalgebra is a left H -comodule (C, ρ) , where C is a coalgebra over k , such that $c_{(-1)} \epsilon(c_{(0)}) = \epsilon(c)1$ and

$$c_{(1)(-1)} c_{(2)(-1)} \otimes c_{(1)(0)} \otimes c_{(2)(0)} = c_{(-1)} \otimes c_{(0)(1)} \otimes c_{(0)(2)}$$

for all $c \in C$. If (C, ρ) is a left H -comodule coalgebra then the tensor product $C \otimes H$ of vector spaces has a coalgebra structure, referred to as the smash coproduct, defined by $\epsilon_{C \otimes H} = \epsilon_C \otimes \epsilon_H$ and

$$(1.2) \quad \Delta(c \otimes h) = (c_{(1)} \otimes c_{(2)(-1)} h_{(1)}) \otimes (c_{(2)(0)} \otimes h_{(2)})$$

for all $c \in C$ and $h \in H$. The usual notation for this coalgebra is $C \sharp H$. The tensor $c \otimes h$ is written $c \sharp h$.

Let $A = B \times H$ be a biproduct. Generally B with its algebra and coalgebra structure is not a bialgebra over k . However:

$$(1.3) \quad \epsilon \in \text{Alg}(B, k), \quad \Delta(1) = 1$$

and

$$(1.4) \quad \Delta(bb') = b_{(1)}(b_{(2)(-1)} \cdot b'_{(1)}) \otimes b_{(2)(0)} b'_{(2)}$$

for all $b, b' \in B$. When B is a left H -module algebra and coalgebra, is a left H -comodule algebra and coalgebra, (1.3) and (1.4) are satisfied,

$$(1.5) \quad h_{(1)} m_{(-1)} \otimes h_{(2)} \cdot m_{(0)} = (h_{(1)} \cdot m)_{(-1)} h_{(2)} \otimes (h_{(1)} \cdot m)_{(0)}$$

holds for all $h \in H$ and $m \in B$, and Id_B has a convolution inverse, then the vector space $A = B \otimes H$ is a Hopf algebra with the smash product algebra structure and the smash coproduct coalgebra structure. The Hopf algebra A is called the biproduct of B and H and is denoted $A = B \times H$. Tensors $b \otimes h$ are denoted $b \times h$.

Let $A = B \times H$ be the biproduct of B and H . Define $\pi : A \rightarrow H$ by $\pi(b \times h) = \epsilon(b)h$ for $b \in B$, $h \in H$ and $j : H \rightarrow A$ by $j(h) = 1 \times h$ for $h \in H$. Observe that π and j are Hopf algebra maps and $\pi \circ j = \text{Id}_H$. The map π is referred to as a Hopf algebra projection of A onto H .

Conversely, if A and H are Hopf algebras over k and $\pi : A \rightarrow H$, $j : H \rightarrow A$ are Hopf algebra maps which satisfy $\pi \circ j = \text{Id}_H$ then $A \simeq B \times H$ for some B . See [11] which covers all the details for this section.

Throughout this paper biproducts will be Hopf algebras over k .

2. CERTAIN CATEGORIES ASSOCIATED WITH BIPRODUCTS

Let H be a Hopf algebra over the field k . We denote by $\mathcal{C}_{\text{proj}}$ the category whose objects are quadruples (A, H, π, j) , where A is a Hopf algebra over k and $\pi : A \rightarrow H$, $j : H \rightarrow A$ are Hopf algebra maps which satisfy $\pi \circ j = \text{Id}_H$. Morphisms are pairs $(F, f) : (A, H, \pi, j) \rightarrow (A', H', \pi', j')$, where $F : A \rightarrow A'$ and $f : H \rightarrow H'$ are Hopf algebra maps such that the diagrams

$$(2.1) \quad \begin{array}{ccc} A & \xrightarrow{F} & A' \\ \pi \downarrow & & \downarrow \pi' \\ H & \xrightarrow{f} & H' \end{array} \quad \text{and} \quad \begin{array}{ccc} A & \xrightarrow{F} & A' \\ j \uparrow & & \uparrow j' \\ H & \xrightarrow{f} & H' \end{array}$$

commute. The composition of morphisms is given by the composition of components. For an object (A, H, π, j) of $\mathcal{C}_{\text{proj}}$ we let $\text{End}_{\text{Hopf}}(A, H, \pi, j)$ be the set of all Hopf algebra endomorphisms F of A such that the diagrams

$$(2.2) \quad \begin{array}{ccc} A & \xrightarrow{F} & A \\ & \searrow \pi & \swarrow \pi \\ & H & \end{array} \quad \text{and} \quad \begin{array}{ccc} A & \xrightarrow{F} & A \\ & \swarrow j & \searrow j \\ & H & \end{array}$$

commute. Thus $\text{End}_{\text{Hopf}}(A, H, \pi, j)$ is the set of all F such that (F, Id_H) is an endomorphism of (A, H, π, j) . Observe that $\text{End}_{\text{Hopf}}(A, H, \pi, j)$ is a monoid under function composition. The units of this monoid form the set $\text{Aut}_{\text{Hopf}}(A, H, \pi, j)$ of all Hopf algebra automorphisms F of A such that the

diagrams of (2.2) commute. It is a subgroup of the group $\text{Aut}_{\text{Hopf}}(A)$ of all Hopf algebra automorphisms of A group under composition.

As it turns out $\text{Aut}_{\text{Hopf}}(A, H, \pi, j)$ is a bit too special. We will consider a less restrictive setting in our study of endomorphisms of biproducts by ignoring the map j .

Let $\mathcal{C}'_{\text{proj}}$ be the category whose objects are triples (A, H, π) which come from objects (A, H, π, j) of $\mathcal{C}_{\text{proj}}$. Morphisms of the category $\mathcal{C}'_{\text{proj}}$ are pairs $(F, f) : (A, H, \pi) \rightarrow (A', H', \pi')$, where $F : A \rightarrow A'$ and $f : H \rightarrow H'$ are Hopf algebra maps such that the first diagram of (2.1) commutes. Again, composition of morphisms is given by composition of components.

For an object (A, H, π) of $\mathcal{C}'_{\text{proj}}$ let $\text{End}_{\text{Hopf}}(A, H, \pi)$ be the monoid of all Hopf algebra endomorphisms F of A such that the first diagram of (2.2) commutes and let $\text{Aut}_{\text{Hopf}}(A, H, \pi)$ be its set of units. Thus $\text{Aut}_{\text{Hopf}}(A, H, \pi)$ is the group of Hopf algebra automorphisms F of A such that $\pi \circ F = \pi$ under composition.

In the context of a fixed H we will simplify symbolism by dropping the H in the notation for the two monoids and two groups defined above. Thus we will write $\text{Aut}_{\text{Hopf}}(A, \pi, j)$ for $\text{Aut}_{\text{Hopf}}(A, H, \pi, j)$ and $\text{Aut}_{\text{Hopf}}(A, \pi)$ for $\text{Aut}_{\text{Hopf}}(A, H, \pi)$.

This paper characterizes elements of $\text{End}_{\text{Hopf}}(A, \pi)$; in particular elements of $\text{Aut}_{\text{Hopf}}(A, \pi)$. Some of them arise from the (left-left) Yetter-Drinfel'd category ${}^H_H\mathcal{YD}$ in terms of which $A = B \times H$ is naturally understood.

The objects of ${}^H_H\mathcal{YD}$ are triples (M, \cdot, ρ) , where (M, \cdot) is a left H -module and (M, ρ) is a left H -comodule, such that (1.5) holds for all $h \in H$ and $m \in M$. Morphisms are functions $f : M \rightarrow N$ of objects which are left H -module and left H -comodule maps. Multiplication of morphisms is function composition. If $A = B \times H$ is a biproduct which is a Hopf algebra over k then B is a Hopf algebra of ${}^H_H\mathcal{YD}$. Conversely, if B is a Hopf algebra of ${}^H_H\mathcal{YD}$ the biproduct $A = B \times H$ is defined and is a Hopf algebra over k .

The category ${}^H_H\mathcal{YD}$ plays a minor role in this paper. Let B be a Hopf algebra of ${}^H_H\mathcal{YD}$. For Theorem 2 we will need a description of the monoid of Hopf algebra endomorphisms $\text{End}_{\mathcal{YD}-\text{Hopf}}(B)$. Recall B is an algebra and coalgebra over k . The elements of $\text{End}_{\mathcal{YD}-\text{Hopf}}(B)$ are those linear endomorphisms of B which are algebra and coalgebra maps and also maps of left H -modules and comodules. $\text{Aut}_{\mathcal{YD}-\text{Hopf}}(B)$ is the group of units of this monoid under function composition.

The reader is encouraged to consult basic references [6, 7, 15] for Yetter-Drinfel'd categories. See [9, 12] also.

3. FACTORIZATION OF CERTAIN BIPRODUCT ENDOMORPHISMS

Throughout this section H is a Hopf algebra with antipode S and $A = B \times H$ is a biproduct which is a Hopf algebra over k . Let $F \in \text{End}_{\text{Hopf}}(A, \pi)$. The purpose of this section is to show F has a factorization closely related to the factors B and H .

Recall from Section 1 that $\pi : A \longrightarrow H$ defined by $\pi(b \times h) = \epsilon(b)h$ for $b \in B$, $h \in H$ and $j : H \longrightarrow A$ defined by $j(h) = 1 \times h$ for $h \in H$ are Hopf algebra maps which satisfy $\pi \circ j = \text{Id}_H$. Likewise we define $\Pi : A \longrightarrow B$ and $J : B \longrightarrow A$ by $\Pi(b \times h) = b\epsilon(h)$ for $b \in B$, $h \in H$ and $J(b) = b \times 1$ for $b \in B$. Note that $\Pi \circ J = \text{Id}_B$. There is a fundamental relationship between these four maps given by

$$(3.1) \quad J \circ \Pi = \text{Id}_A \star (j \circ S \circ \pi).$$

The factorization of F is given in terms of $F_L : B \longrightarrow B$ and $F_R : H \longrightarrow B$ defined by

$$(3.2) \quad F_L = \Pi \circ F \circ J \quad \text{and} \quad F_R = \Pi \circ F \circ j.$$

Lemma 1. *Let $F \in \text{End}_{\text{Hopf}}(A, \pi)$. Then:*

- (a) $F_L(b) \times 1 = F(b \times 1)$ for all $b \in B$.
- (b) $F_R(h) \times 1 = F(1 \times h_{(1)})(1 \times S(h_{(2)}))$ for all $h \in H$.
- (c) $F(b \times h) = F_L(b)F_R(h_{(1)}) \times h_{(2)}$ for all $b \in B$ and $h \in H$.

PROOF: We need to calculate $J \circ \Pi \circ F$. Let $b \in B$ and $h \in H$. We use (3.1) to compute

$$\begin{aligned} (J \circ \Pi)(F(b \times h)) &= F((b \times h)_{(1)})((j \circ S \circ \pi)(F((b \times h)_{(2)}))) \\ &= F((b \times h)_{(1)})((j \circ S \circ \pi)((b \times h)_{(2)})) \\ &= F(b_{(1)} \times b_{(2)(-1)}h_{(1)})((j \circ S \circ \pi)(b_{(2)(0)} \times h_{(2)})) \\ &= F(b_{(1)} \times b_{(2)(-1)}\epsilon(b_{(2)(0)})h_{(1)})(1 \times S(h_{(2)})) \\ &= F(b_{(1)} \times \epsilon(b_{(2)})h_{(1)})(1 \times S(h_{(2)})) \\ &= F(b \times h_{(1)})(1 \times S(h_{(2)})). \end{aligned}$$

Thus

$$(J \circ \Pi \circ F)(b \times h) = F(b \times h_{(1)})(1 \times S(h_{(2)}))$$

for all $b \in B$ and $h \in H$. Parts (a) and (b) follow from these equations. As for part (c), we use parts (a) and (b) to calculate

$$\begin{aligned} F(b \times h) &= F((b \times 1)(1 \times h)) \\ &= F(b \times 1)F(1 \times h) \\ &= F(b \times 1)F(1 \times h_{(1)})(1 \times S(h_{(2)}))(1 \times h_{(3)}) \\ &= (F_L(b) \times 1)(F_R(h_{(1)}) \times 1)(1 \times h_{(2)}) \\ &= F_L(b)F_R(h_{(1)}) \times h_{(2)} \end{aligned}$$

for all $b \in B$ and $h \in H$. □

By parts (a) and (b) of the preceding lemma:

$$(3.3) \quad (\text{Id}_A)_L = \text{Id}_B \quad \text{and} \quad (\text{Id}_A)_R = \eta \circ \epsilon.$$

Since $F_L(1) = 1$ by part (a) of Lemma 1, by part (c) of the same:

$$(3.4) \quad F(1 \times h) = F_R(h_{(1)}) \times h_{(2)}$$

for all $h \in H$. We are now able to compute the factors of a composite.

Corollary 1. *Let $F, G \in \text{End}_{\text{Hopf}}(A, \pi)$. Then:*

- (a) $(F \circ G)_L = F_L \circ G_L$.
- (b) $(F \circ G)_R = (F_L \circ G_R) \star F_R$.

PROOF: Let $b \in B$. Then $(F \circ G)_L(b) \times 1 = F_L(G_L(b)) \times 1$ follows by part (a) of Lemma 1. Part (a) is established. Let $h \in H$. Using (3.4), parts (a) and (c) of Lemma 1, and the fact the F is multiplicative, we note that

$$\begin{aligned}
 (F \circ G)_R(h_{(1)}) \times h_{(2)} &= (F \circ G)(1 \times h) \\
 &= F(G(1 \times h)) \\
 &= F(G_R(h_{(1)}) \times h_{(2)}) \\
 &= F(G_R(h_{(1)}) \times 1)F(1 \times h_{(2)}) \\
 &= (F_L(G_R(h_{(1)})) \times 1)(F_R(h_{(2)}) \times h_{(3)}) \\
 &= F_L(G_R(h_{(1)}))F_R(h_{(2)}) \times h_{(3)}
 \end{aligned}$$

from which $(F \circ G)_R(h) = F_L(G_R(h_{(1)}))F_R(h_{(2)})$ follows. We have shown part (b) holds. \square

By virtue of Lemma 1, to characterize F is a matter of characterizing F_L and F_R . Note in particular part (e) of the following describes a commutation relation between F_L and F_R .

Lemma 2. *Let $F \in \text{End}_{\text{Hopf}}(A, \pi)$. Then:*

- (a) $F_L : B \longrightarrow B$ is an algebra endomorphism.
- (b) $\epsilon \circ F_L = \epsilon$.
- (c) $\Delta(F_L(b)) = F_L(b_{(1)})F_R(b_{(2)(-1)}) \otimes F_L(b_{(2)(0)})$ for all $b \in B$.
- (d) $\rho(F_L(b)) = b_{(-1)} \otimes F_L(b_{(0)})$ for all $b \in B$.
- (e) $F_L(h_{(1)} \cdot b)F_R(h_{(2)}) = F_R(h_{(1)})(h_{(2)} \cdot F_L(b))$ for all $h \in H$ and $b \in B$.

PROOF: We first show part (a). That $F(B \times 1) \subseteq B \times 1$ follows by part (a) of Lemma 1. Let $F_r : B \times 1 \longrightarrow B \times 1$ be the map induced by restriction of F . The map J thought of as $J : B \longrightarrow B \times 1$ is an algebra isomorphism. Thus $F_L = J^{-1} \circ F_r \circ J$ is an algebra map since it is the composition of such. Part (b) follows since $\epsilon \circ J = \epsilon$ and F is a coalgebra map. Let $b \in B$. To show part (c) we compute the coproduct of $F_L(b) \times 1 = F(b \times 1)$ in two ways. First of all

$$\Delta(F_L(b) \times 1) = (F_L(b)_{(1)} \times F_L(b)_{(2)(-1)}) \otimes (F_L(b)_{(2)(0)} \times 1)$$

and secondly, since F is a coalgebra map,

$$\begin{aligned}
 \Delta(F(b \times 1)) &= F((b \times 1)_{(1)}) \otimes F((b \times 1)_{(2)}) \\
 &= F(b_{(1)} \times b_{(2)(-1)}) \otimes F(b_{(2)(0)} \times 1) \\
 &= (F_L(b_{(1)})F_R(b_{(2)(-1)(1)}) \times b_{(2)(-1)(2)}) \otimes (F_L(b_{(2)(0)}) \times 1);
 \end{aligned}$$

the last equation follows by part (c) of Lemma 1. We obtain part (c) by applying ϵ to the second and fourth factors to the two expressions for the coproduct. Noting that $\epsilon \circ F_R = \epsilon$, which follows by (3.4), we use part (b) to obtain part (d) by applying ϵ to the first and fourth factors of the same coproduct expressions.

It remains to show part (e). For $b \in B$ and $h \in H$ we have

$$F((1 \times h)(b \times 1)) = F(h_{(1)} \cdot b \times h_{(2)}) = F_L(h_{(1)} \cdot b)F_R(h_{(2)}) \times h_{(3)}$$

by part (c) of Lemma 1. On the other hand, since F is an algebra map we use (3.4) and part (a) of Lemma 1 to compute

$$\begin{aligned} F((1 \times h)(b \times 1)) &= F(1 \times h)F(b \times 1) \\ &= (F_R(h_{(1)}) \times h_{(2)})(F_L(b) \times 1) \\ &= F_R(h_{(1)})(h_{(2)} \cdot F_L(b)) \times h_{(3)}. \end{aligned}$$

Applying ϵ to the second factor of both expressions for $F((1 \times h)(b \times 1))$ we obtain part (e). \square

As the reader might suspect, whether or not F_L is a coalgebra map is explained in terms of F_R .

Corollary 2. *Let $F \in \text{End}_{\text{Hopf}}(A, \pi)$. Then F_L is a coalgebra map if and only if $F_R(c_{(-1)}) \otimes c_{(0)} = 1 \otimes c$ for all $c \in \text{Im}(F_L)$.*

PROOF: Suppose $F_R(c_{(-1)}) \otimes c_{(0)} = 1 \otimes c$ for all $c \in \text{Im}(F_L)$. Then by parts (c) and (d) of Lemma 2 we have

$$\begin{aligned} \Delta(F_L(b)) &= F_L(b_{(1)})F_R(b_{(2)(-1)}) \otimes F_L(b_{(2)(0)}) \\ &= F_L(b_{(1)})F_R(F_L(b_{(2)})_{(-1)}) \otimes F_L(b_{(2)})_{(0)} \\ &= F_L(b_{(1)})1 \otimes F_L(b_{(2)}) \end{aligned}$$

for all $b \in B$. This calculation and part (b) of Lemma 2 imply that F_L is a coalgebra map.

Conversely, suppose that F_L is a coalgebra map. Using parts (a), (c), and (d) of Lemma 2 we compute for all $b \in B$ that

$$\begin{aligned} F_R(F_L(b)_{(-1)}) \otimes F_L(b)_{(0)} &= F_L(\epsilon(b_{(1)})1)F_R(F_L(b_{(2)})_{(-1)}) \otimes F_L(b_{(2)})_{(0)} \\ &= F_L(S(b_{(1)})b_{(2)})F_R(b_{(3)(-1)}) \otimes F_L(b_{(3)(0)}) \\ &= F_L(S(b_{(1)}))F_L(b_{(2)})F_R(b_{(3)(-1)}) \otimes F_L(b_{(3)(0)}) \\ &= F_L(S(b_{(1)}))F_L(b_{(2)})_{(1)} \otimes F_L(b_{(2)})_{(2)} \\ &= F_L(S(b_{(1)}))F_L(b_{(2)}) \otimes F_L(b_{(3)}) \\ &= F_L(S(b_{(1)})b_{(2)}) \otimes F_L(b_{(3)}) \\ &= F_L(1) \otimes F_L(b) \\ &= 1 \otimes F_L(b). \end{aligned}$$

We have shown that $F_R(c_{(-1)}) \otimes c_{(0)} = 1 \otimes c$ for all $c \in \text{Im}(F_L)$. \square

Lemma 3. *Let $F \in \text{End}_{\text{Hopf}}(A, \pi)$. Then:*

- (a) $F_R(hh') = F_R(h_{(1)})(h_{(2)} \cdot F_R(h'))$ for all $h, h' \in H$.
- (b) $F_R(1) = 1$.
- (c) $F_R : H \rightarrow B$ is a coalgebra map.
- (d) $\rho(F_R(h)) = h_{(1)}S(h_{(3)}) \otimes F_R(h_{(2)})$ for all $h \in H$.

PROOF: By (3.4) we have $F(1 \times h) = F_R(h_{(1)}) \times h_{(2)}$ for all $h \in H$. Since F is an algebra map, $1 \times 1 = F(1 \times 1) = F_R(1) \times 1$ which implies $F_R(1) = 1$. We have established part (b). As for part (a), for $h, h' \in H$ we calculate on one hand

$$F(1 \times hh') = F_R(h_{(1)}h'_{(1)}) \times h_{(2)}h'_{(2)}$$

and on the other

$$\begin{aligned} F(1 \times hh') &= F((1 \times h)(1 \times h')) \\ &= F(1 \times h)F(1 \times h') \\ &= (F_R(h_{(1)}) \times h_{(2)})(F_R(h'_{(1)}) \times h'_{(2)}) \\ &= F_R(h_{(1)})(h_{(2)} \cdot F_R(h'_{(1)})) \times h_{(3)}h'_{(2)}. \end{aligned}$$

Applying ϵ to the second factor of both expressions for $F(1 \times hh')$ establishes part (a).

Let $h \in H$. To show parts (c) and (d) we compute $\Delta(F(1 \times h))$ in two ways. Since F and j are coalgebra maps

$$\Delta(F(1 \times h)) = F(1 \times h_{(1)}) \otimes F(1 \times h_{(2)}) = (F_R(h_{(1)}) \times h_{(2)}) \otimes (F_R(h_{(3)}) \times h_{(4)}).$$

On the other hand

$$\begin{aligned} \Delta(F(1 \times h)) &= \Delta(F_R(h_{(1)}) \times h_{(2)}) \\ &= (F_R(h_{(1)})_{(1)} \times F_R(h_{(1)})_{(2)(-1)}h_{(2)}) \otimes (F_R(h_{(1)})_{(2)(0)} \times h_{(3)}). \end{aligned}$$

Applying ϵ to the second and fourth factors of the expressions for $\Delta(F(1 \times h))$ gives $F_R(h_{(1)}) \otimes F_R(h_{(2)}) = \Delta(F_R(h))$ and, since $\epsilon \circ F_R = \epsilon$, to the first and fourth gives $h_{(1)} \otimes F_R(h_{(2)}) = F_R(h_{(1)})_{(-1)}h_{(2)} \otimes F_R(h_{(1)})_{(0)}$. Therefore

$$\rho(F_R(h)) = F_R(h_{(1)})_{(-1)}h_{(2)}S(h_{(3)}) \otimes F_R(h_{(1)})_{(0)} = h_{(1)}S(h_{(3)}) \otimes F_R(h_{(2)}).$$

We have established parts (c) and (d). \square

Corollary 3. *Let $F \in \text{End}_{\text{Hopf}}(A, \pi)$. Then:*

- (a) F_L is a left H -module map if and only if the condition

$$F_L(h_{(1)} \cdot b)F_R(h_{(2)}) = F_R(h_{(1)})F_L(h_{(2)} \cdot b)$$

holds for all $h \in H$ and $b \in B$.

- (b) If B is commutative and H is cocommutative then F_L is a left H -module map.

PROOF: Part (b) follows immediately from part (a). To show part (a), we first note if F_L is a map of left H -modules then the condition follows by part (e) of Lemma 2. Suppose the condition holds. Now F_R is a coalgebra map by part (c) of Lemma 3. Using this fact and part (e) of Lemma 2, observe for all $h \in H$ and $b \in B$ that

$$\begin{aligned}
h \cdot F_L(b) &= \epsilon(F_R(h_{(1)}))(h_{(2)} \cdot F_L(b)) \\
&= S(F_R(h_{(1)}))F_R(h_{(2)})(h_{(3)} \cdot F_L(b)) \\
&= S(F_R(h_{(1)}))F_L(h_{(2)} \cdot b)F_R(h_{(3)}) \\
&= S(F_R(h_{(1)}))F_R(h_{(2)})F_L(h_{(3)} \cdot b) \\
&= \epsilon(F_R(h_{(1)}))F_L(h_{(2)} \cdot b) \\
&= F_L(h \cdot b)
\end{aligned}$$

which shows that F_L is a left H -module map. \square

Corollary 4. *Let $F \in \text{End}_{\text{Hopf}}(A, \pi)$. Then F_R is an algebra map if and only if $h \cdot F_R(h') = \epsilon(h)F_R(h')$ for all $h, h' \in H$.*

PROOF: First of all $F_R(1) = 1$ by part (b) of Lemma 3. If the condition $h \cdot F_R(h') = \epsilon(h)F_R(h')$ holds for all $h, h' \in H$ then $F_R(hh') = F_R(h)F_R(h')$ for all $h, h' \in H$ by part (a) of Lemma 3. Thus F_R is an algebra map.

Suppose F_R is an algebra map and let $h, h' \in H$. Now F_R is a coalgebra map by part (c) of Lemma 3. Using this fact and part (a) of the same again

$$\begin{aligned}
\epsilon(h)F_R(h') &= S(F_R(h_{(1)}))F_R(h_{(2)})F_R(h') \\
&= S(F_R(h_{(1)}))F_R(h_{(2)}h') \\
&= S(F_R(h_{(1)}))F_R(h_{(2)})(h_{(3)} \cdot F_R(h')) \\
&= \epsilon(h_{(1)})h_{(2)} \cdot F_R(h') \\
&= h \cdot F_R(h').
\end{aligned}$$

\square

Corollary 5. *Let $F \in \text{End}_{\text{Hopf}}(A, \pi)$. Then F_R has a convolution inverse J_R defined by $J_R(h) = h_{(1)} \cdot F_R(S(h_{(2)}))$ for all $h \in H$.*

PROOF: Let $h \in H$. Then by parts (a) and (b) of Lemma 3 we have

$$\begin{aligned}
F_R \star J_R(h) &= F_R(h_{(1)})(h_{(2)} \cdot F_R(S(h_{(3)}))) \\
&= F_R(h_{(1)})S(h_{(2)}) \\
&= F_R(\epsilon(h)1) \\
&= \epsilon(h)1
\end{aligned}$$

and using the fact that B is a left H -module algebra we have

$$\begin{aligned}
J_R \star F_R(h) &= (h_{(1)} \cdot F_R(S(h_{(2)}))) F_R(h_{(3)}) \\
&= h_{(1)} \cdot (F_R(S(h_{(3)}))(S(h_{(2)}) \cdot F_R(h_{(4)}))) \\
&= h_{(1)} \cdot (F_R(S(h_{(2)}))_{(1)})(S(h_{(2)})_{(2)} \cdot F_R(h_{(3)})) \\
&= h_{(1)} \cdot (F_R(S(h_{(2)})h_{(3)})) \\
&= h_{(1)} \cdot (F_R(\epsilon(h)1)) \\
&= h \cdot F_R(1) \\
&= h \cdot 1 \\
&= \epsilon(h)1.
\end{aligned}$$

□

We now characterize $\text{End}_{\text{Hopf}}(A, \pi)$ and $\text{Aut}_{\text{Hopf}}(A, \pi)$.

Theorem 1. *Let $A = B \times H$ be a biproduct and $\pi : A \rightarrow H$ be the projection from A onto H and let $\mathcal{F}_{B,H}$ be the set of pairs (f, g) , where $f : B \rightarrow B$ and $g : H \rightarrow B$ are maps satisfy the conclusions of Lemma 2 and Lemma 3 for F_L and F_R respectively. Then:*

- (a) *The function $\mathcal{F}_{B,H} \rightarrow \text{End}_{\text{Hopf}}(A, \pi)$, described by $(f, g) \mapsto F$, where $F(b \times h) = f(b)g(h_{(1)}) \times h_{(2)}$ for all $b \in B$ and $h \in H$, is a bijection. Furthermore $F_L = f$ and $F_R = g$.*
- (b) *Suppose $(f, g) \in \mathcal{F}_{B,H}$. Then $F \in \text{Aut}_{\text{Hopf}}(A, \pi)$ if and only if f is a bijection.*

PROOF: Assume the function of part (a) is well-defined. We first observe that $F \mapsto (\Pi \circ F \circ J, \Pi \circ F \circ j)$ describes its inverse; see (3.2). In light of the preceding results, to complete the proof of part (a) we need only show that elements of $\mathcal{F}_{B,H}$ give rise to elements of $\text{End}_{\text{Hopf}}(A, \pi)$ as indicated. Let $(f, g) \in \mathcal{F}_{B,H}$ and let F be defined as in part (a). As the reader might suspect, the proof that $F \in \text{End}_{\text{Hopf}}(A, \pi)$ is somewhat tedious. We will use Lemmas 1, 2, and 3 without particular reference initially.

It is easy to see that $\pi \circ F = \pi$. Note that $F(1 \times 1) = f(1)g(1) \times 1 = 1 \times 1$ and

$$\begin{aligned}
\epsilon(F(b \times h)) &= \epsilon(f(b)g(h_{(1)}) \times h_{(2)}) \\
&= \epsilon(f(b)g(h_{(1)}))\epsilon(h_{(2)}) \\
&= \epsilon(f(b)g(h)) \\
&= \epsilon(f(b))\epsilon(g(h)) \\
&= \epsilon(b)\epsilon(h)
\end{aligned}$$

for $b \in B$ and $h \in H$ which means $\epsilon \circ F = \epsilon$. That $F_L = f$ and $F_R = g$ is easy to see.

Let $b, b' \in B$ and $h, h' \in H$. Then

$$\begin{aligned}
& F((b \times h)(b' \times h')) \\
&= F(b(h_{(1)} \cdot b') \times h_{(2)} h') \\
&= f(b(h_{(1)} \cdot b'))g(h_{(2)} h'_{(1)}) \times h_{(3)} h'_{(2)} \\
&= f(b)f(h_{(1)} \cdot b')g(h_{(2)} h'_{(1)}) \times h_{(3)} h'_{(2)} \\
&= f(b)f(h_{(1)} \cdot b')g(h_{(2)})(h_{(3)} \cdot g(h'_{(1)})) \times h_{(4)} h'_{(2)} \\
&= f(b)g(h_{(1)})(h_{(2)} \cdot f(b'))(h_{(3)} \cdot g(h'_{(1)})) \times h_{(4)} h'_{(2)} \\
&= f(b)g(h_{(1)})(h_{(2)} \cdot (f(b')g(h'_{(1)}))) \times h_{(3)} h'_{(2)} \\
&= (f(b)g(h_{(1)}) \times h_{(2)})(f(b')g(h'_{(1)}) \times h'_{(2)}) \\
&= F(b \times h)F(b' \times h').
\end{aligned}$$

Therefore F is an algebra map. Using (1.2) and (1.4) we obtain:

$$\begin{aligned}
& \Delta(F(b \times h)) \\
&= \Delta(f(b)g(h_{(1)}) \times h_{(2)}) \\
&= (f(b)g(h_{(1)}))_{(1)} \times (f(b)g(h_{(1)}))_{(2)(-1)} h_{(2)} \\
&\quad \otimes ((f(b)g(h_{(1)}))_{(2)(0)} \times h_{(3)}) \\
&= (f(b)_{(1)}(f(b)_{(2)(-1)} \cdot g(h_{(1)}))_{(1)}) \times (f(b)_{(2)(0)}g(h_{(1)}_{(2)})_{(-1)}h_{(2)}) \\
&\quad \otimes ((f(b)_{(2)(0)}g(h_{(1)}_{(2)})_{(0)} \times h_{(3)}).
\end{aligned}$$

Since g is a coalgebra map and B is a left H -comodule algebra the last expression

$$\begin{aligned}
&= (f(b)_{(1)}(f(b)_{(2)(-1)} \cdot g(h_{(1)})) \times (f(b)_{(2)(0)}g(h_{(2)}))_{(-1)}h_{(3)}) \\
&\quad \otimes ((f(b)_{(2)(0)}g(h_{(2)}))_{(0)} \times h_{(4)}) \\
&= (f(b)_{(1)}(f(b)_{(2)(-1)} \cdot g(h_{(1)})) \times f(b)_{(2)(0)(-1)}g(h_{(2)})_{(-1)}h_{(3)}) \\
&\quad \otimes (f(b)_{(2)(0)(0)}g(h_{(2)})_{(0)} \times h_{(4)}).
\end{aligned}$$

Using part (d) of Lemma 3 and part (c) of Lemma 2 the last expression

$$\begin{aligned}
&= (f(b)_{(1)}(f(b)_{(2)(-1)} \cdot g(h_{(1)})) \times f(b)_{(2)(0)(-1)}h_{(2)}S(h_{(4)})h_{(5)}) \\
&\quad \otimes (f(b)_{(2)(0)(0)}g(h_{(3)}) \times h_{(6)}) \\
&= (f(b)_{(1)}(f(b)_{(2)(-1)} \cdot g(h_{(1)})) \times f(b)_{(2)(0)(-1)}h_{(2)}) \\
&\quad \otimes (f(b)_{(2)(0)(0)}g(h_{(3)}) \times h_{(4)}) \\
&= (f(b_{(1)})g(b_{(2)(-1)})(f(b_{(2)(0)})_{(-1)} \cdot g(h_{(1)})) \times f(b_{(2)(0)})_{(0)(-1)}h_{(2)}) \\
&\quad \otimes (f(b_{(2)(0)})_{(0)(0)}g(h_{(3)}) \times h_{(4)}).
\end{aligned}$$

Using part (d) of Lemma 2, the coassociative comodule axiom, and part (a) of Lemma 3 the last expression

$$\begin{aligned}
&= (f(b_{(1)})g(b_{(2)(-1)})(b_{(2)(0)(-1)} \cdot g(h_{(1)})) \times f(b_{(2)(0)(0)}(-1)h_{(2)}) \\
&\quad \otimes (f(b_{(2)(0)(0)}(0)g(h_{(3)}) \times h_{(4)}) \\
&= (f(b_{(1)})g(b_{(2)(-1)(1)})(b_{(2)(-1)(2)} \cdot g(h_{(1)})) \times f(b_{(2)(0)}(-1)h_{(2)}) \\
&\quad \otimes (f(b_{(2)(0)}(0)g(h_{(3)}) \times h_{(4)}) \\
&= (f(b_{(1)})g(b_{(2)(-1)}h_{(1)}) \times f(b_{(2)(0)}(-1)h_{(2)}) \\
&\quad \otimes (f(b_{(2)(0)}(0)g(h_{(3)}) \times h_{(4)}).
\end{aligned}$$

Using part (d) of Lemma 2, the coassociative comodule axiom again, and (1.2) the last expression

$$\begin{aligned}
&= (f(b_{(1)})g(b_{(2)(-1)}h_{(1)}) \times b_{(2)(0)(-1)}h_{(2)}) \\
&\quad \otimes (f(b_{(2)(0)(0)}g(h_{(3)}) \times h_{(4)}) \\
&= (f(b_{(1)})g(b_{(2)(-1)(1)}h_{(1)}) \times b_{(2)(-1)(2)}h_{(2)}) \\
&\quad \otimes (f(b_{(2)(0)}g(h_{(3)}) \times h_{(4)}) \\
&= F(b_{(1)} \times b_{(2)(-1)}h_{(1)}) \otimes F(b_{(2)(0)} \times h_{(2)}) \\
&= F((b \times h)_{(1)}) \otimes F((b \times h)_{(2)}).
\end{aligned}$$

We have shown that $\Delta \circ F = (F \otimes F) \circ \Delta$. Therefore F is a coalgebra map and consequently is a bialgebra map. Since bialgebra maps of Hopf algebras are Hopf algebra maps, the proof of part (a) is complete.

As for part (b), suppose $F \in \text{Aut}_{\text{Hopf}}(A, \pi)$. Then F_L and $(F^{-1})_L$ are inverses by (3.3) and part (a) of Corollary 1. Thus F_L is bijective and $(F_L)^{-1} = (F^{-1})_L$.

Conversely, suppose that $F \in \text{End}_{\text{Hopf}}(A, \pi)$ and F_L is bijective. Set $G_L = (F_L)^{-1}$. Now F_R has a convolution inverse J_R by Corollary 5. Set $G_R = G_L \circ J_R = (F_L)^{-1} \circ J_R$ and define $G \in \text{End}(A)$ by $G(b \times h) = G_L(b)G_R(h_{(1)}) \times h_{(2)}$ for all $b \in B$ and $h \in H$. Since G_L is an algebra map we compute

$$\begin{aligned}
G(F(b \times h)) &= G(F_L(b)F_R(h_{(1)}) \times h_{(2)}) \\
&= G_L(F_L(b)F_R(h_{(1)}))G_R(h_{(2)}) \otimes h_{(3)} \\
&= G_L(F_L(b)F_R(h_{(1)}))G_L(J_R(h_{(2)})) \otimes h_{(3)} \\
&= bG_L(F_R(h_{(1)})J_R(h_{(2)})) \otimes h_{(3)} \\
&= bG_L((F_R \star J_R)(h_{(1)})) \times h_{(2)} \\
&= bG_L(\epsilon(h_{(1)})1) \times h_{(2)} \\
&= b \times h
\end{aligned}$$

and

$$\begin{aligned}
F(G(b \times h)) &= F(G_L(b)G_R(h_{(1)}) \times h_{(2)}) \\
&= F_L(G_L(b)G_R(h_{(1)}))F_R(h_{(2)}) \otimes h_{(3)} \\
&= F_L(G_L(b)(F_L)^{-1}(J_R(h_{(1)})))F_R(h_{(2)}) \otimes h_{(3)} \\
&= b(J_R(h_{(1)})F_R(h_{(2)})) \times h_{(3)} \\
&= b((J_R \star F_R)(h_{(1)})) \times h_{(2)} \\
&= b(\epsilon(h_{(1)})1) \times h_{(2)} \\
&= b \times h.
\end{aligned}$$

We have shown $G \circ F = \text{Id}_A = F \circ G$. Therefore F is bijective and the proof of part (b) is complete. \square

Apropos of the preceding theorem, let $\mathcal{F}_{B,H}^\bullet$ denote the set of $(f, g) \in \mathcal{F}_{B,H}$ such that f is bijective. Then the correspondence of part (a) induces a bijection $\mathcal{F}_{B,H}^\bullet \longrightarrow \text{Aut}_{\text{Hopf}}(A, \pi)$.

When $F(1 \times H) \subseteq 1 \times H$ the structure of F is particularly simple.

Proposition 1. *Let $F \in \text{End}_{\text{Hopf}}(A, \pi)$. Then the following conditions are equivalent:*

- (a) $F(1 \times H) \subseteq 1 \times H$.
- (b) $F_R(h) \in k1$ for all $h \in H$.
- (c) $F_R(h) = \epsilon(h)1$ for all $h \in H$.
- (d) $F_R = \eta \circ \epsilon$.
- (e) $F(b \times h) = F_L(b) \times h$ for all $b \in B$ and $h \in H$.
- (f) $F(1 \times h) = 1 \times h$ for all $h \in H$.

If $F \in \text{Aut}_{\text{Hopf}}(A, \pi)$ any of these conditions implies $F_L \in \text{Aut}_{\mathcal{YD}\text{-Hopf}}(B)$.

PROOF: We first show part (a) implies part (b) implies part (c). Suppose $F(1 \times H) \subseteq 1 \times H$. Then $F_R(H) \subseteq k1$ by (3.4). Thus $F_R(h) = \epsilon(h)1$ for all $h \in H$ since $\epsilon \circ F_R = \epsilon$. Part (d) is an equivalent expression of part (c).

Suppose part (d) holds. Then $F(b \times h) = F_L(b) \times h$ for all $b \in B$ and $h \in H$ by virtue of part (c) of Lemma 1.

We have shown that part (d) implies part (e). Part (e) implies part (f) as $F_L(1) = 1$. Part (f) trivially implies part (a). We have shown the conditions are equivalent. If part (c) holds and $F \in \text{Aut}_{\text{Hopf}}(A, \pi)$ then $F_L \in \text{Aut}_{\mathcal{YD}\text{-Hopf}}(B)$ follows by Lemma 2. \square

Let

$$\text{End}'_{\text{Hopf}}(A, \pi) = \{F \in \text{End}_{\text{Hopf}}(A, \pi) \mid F(1 \times H) \subseteq 1 \times H\}$$

and

$$\text{Aut}'_{\text{Hopf}}(A, \pi) = \text{Aut}_{\text{Hopf}}(A, \pi) \cap \text{End}'_{\text{Hopf}}(A, \pi).$$

Then $\text{End}'_{\text{Hopf}}(A, \pi)$ is a submonoid of $\text{End}_{\text{Hopf}}(A, \pi)$ and $\text{Aut}'_{\text{Hopf}}(A, \pi)$ is a subgroup of $\text{Aut}_{\text{Hopf}}(A, \pi)$. By virtue of the preceding proposition

$$(3.5) \quad \text{End}'_{\text{Hopf}}(A, \pi) = \text{End}_{\text{Hopf}}(A, \pi, j)$$

and

$$(3.6) \quad \text{Aut}'_{\text{Hopf}}(A, \pi) = \text{Aut}_{\text{Hopf}}(A, \pi, j).$$

Most of the proof of the following theorem is established by the preceding proposition. The remainder of the proof is left to the reader.

Theorem 2. *Let $A = B \times H$ be a biproduct. There is an isomorphism of monoids $\text{End}_{\mathcal{YD}\text{-Hopf}}(B) \simeq \text{End}_{\text{Hopf}}(A, \pi, j)$ and an isomorphism of groups $\text{Aut}_{\mathcal{YD}\text{-Hopf}}(B) \simeq \text{Aut}_{\text{Hopf}}(A, \pi, j)$, given by $f \mapsto F$, where $F(b \times h) = f(b) \times h$ for all $b \in B$ and $h \in H$. \square*

There are biproducts found in [9] where $\text{Aut}_{\text{Hopf}}(A, \pi) = \text{Aut}'_{\text{Hopf}}(A, \pi)$, hence $\text{Aut}_{\text{Hopf}}(A, \pi) = \text{Aut}_{\text{Hopf}}(A, \pi, j) \simeq \text{Aut}_{\mathcal{YD}\text{-Hopf}}(B)$ by the preceding theorem.

Theorem 3. *Let $A = B \times H$ be a biproduct. Suppose that the left H -module action on B is trivial and that $k1$ is the only subcoalgebra in the center of B . Then $\text{Aut}_{\text{Hopf}}(A, \pi) = \text{Aut}_{\text{Hopf}}(A, \pi, j) \simeq \text{Aut}_{\mathcal{YD}\text{-Hopf}}(B)$.*

PROOF: Let $F \in \text{Aut}_{\text{Hopf}}(A, \pi)$. In light of Theorem 2 we need only show that $F \in \text{Aut}'_{\text{Hopf}}(A, \pi)$. Now $F_L(b)F_R(h) = F_R(h)F_L(b)$ for all $h \in H$ and $b \in B$ by part (e) of Lemma 2 since the H -module action on B is trivial. It follows that F_L is bijective by part (b) of Theorem 1 since F is an automorphism of A . Now F_R is coalgebra map by part (c) of Lemma 3. Therefore $F_R(H)$ is a subcoalgebra of B in the center of B . By assumption $F_R(H) = k1$. Therefore $F \in \text{Aut}'_{\text{Hopf}}(A, \pi)$ by Proposition 1. \square

The biproduct constructed for the proof of [9, Theorem 6] satisfies the hypothesis of Theorem 3. Here $A = k[\mathcal{G}] \times k[\mathbb{Z}_p]$, where \mathcal{G} is a finite non-abelian simple group and p is a prime integer. $\text{Aut}_{\text{Hopf}}(A, \pi) \simeq \text{Aut}_{\theta}(\mathcal{G})$ which consists of all automorphisms of \mathcal{G} which commute with a certain $\theta \in \text{Aut}_{\text{Group}}(\mathcal{G})$.

4. $\text{Aut}_{\text{Hopf}}(A, \pi)$ AS A SUBGROUP OF A SEMIDIRECT PRODUCT.

Let B be an algebra and C be a coalgebra over k . The group $\mathcal{G}(B) = \text{Aut}_{\text{Group}}(B)$ acts on the convolution algebra $\text{Hom}(C, B)$ by $f \triangleright g = f \circ g$ for all $f \in \mathcal{G}(B)$ and $g \in \text{Hom}(C, B)$. This action satisfies

$$f \triangleright (\eta \circ \epsilon) = \eta \circ \epsilon \quad \text{and} \quad f \triangleright (g \star g') = (f \triangleright g) \star (f \triangleright g')$$

for all $f \in \mathcal{G}(B)$ and $g, g' \in \text{Hom}(C, B)$. Let $\mathcal{U}(C, B)$ be the group of units of the monoid $(\text{Hom}(C, B), \star)$. Then $\mathcal{G} \triangleright \mathcal{U}(C, B) \subseteq \mathcal{U}(C, B)$; thus there is a group homomorphism,

$$\varphi : \mathcal{G}(B) \longrightarrow \text{Aut}_{\text{Group}}(\mathcal{U}(C, B))$$

given by $\varphi(f)(g) = f \triangleright g$ for all $f \in \mathcal{G}(B)$ and $g \in \mathcal{U}(C, B)$. The resulting group $\mathcal{U}(C, B) \rtimes_{\varphi} \mathcal{G}(B)$ has product given by

$$(g, f)(g', f') = (g \star (f \circ g'), f \circ f').$$

Note the action of $\mathcal{G}(B)$ on $\mathcal{U}(C, B)$ by group homomorphisms is also one on $\mathcal{U}(C, B)^{op}$. For a group G the group G^{op} is the group whose underlying set is G and product is given by $g \cdot g' = g'g$ for all $g, g' \in G$. As a result of Theorem 1 and Corollary 1:

Theorem 4. *Suppose $A = B \times H$ is a biproduct and $\pi : A \rightarrow H$ is the projection from A onto H . Then there is a one-one group homomorphism $\text{Aut}_{\text{Hopf}}(A, \pi) \rightarrow \mathcal{U}(H, B)^{op} \rtimes_{\varphi} \mathcal{G}(B)$ which is given by $F \mapsto (F_R, F_L)$ for all $F \in \text{Aut}_{\text{Hopf}}(A, \pi)$. \square*

5. A NORMAL SUBGROUP OF $\text{Aut}_{\text{Hopf}}(A, \pi)$

Let $A = B \times H$ be a biproduct. By part (a) of Lemma 2, Theorem 1, and part (a) of Corollary 1, there is a group homomorphism

$$\nu : \text{Aut}_{\text{Hopf}}(A, \pi) \rightarrow \text{Aut}_{\text{Alg}}(B)$$

defined by $\nu(F) = F_L$ for all $F \in \text{Aut}_{\text{Hopf}}(A, \pi)$. Let $\mathcal{N}(B, H)$ the set of all F_R 's where $F_L = \text{Id}_B$. Then the set of pairs (Id_B, g) , where $g \in \mathcal{N}(B, H)$, is the subset of $\mathcal{F}_{B, H}$ which corresponds to $\text{Ker}(\nu)$ in part (a) of Theorem 1. Therefore $F \in \text{Ker}(\nu)$ if and only if there is a $g \in \mathcal{N}(B, H)$ such that $F(b \times h) = bg(h_{(1)}) \times h_{(2)}$ for all $b \in B$ and $h \in H$.

Proposition 2. *Let $A = B \times H$ be a biproduct. Then:*

- (a) $\mathcal{N}(B, H)$ consists of those maps $g : H \rightarrow B$ which satisfy:
 - (1) $g(b_{(-1)}) \otimes b_{(0)} = 1 \otimes b$ for all $b \in B$;
 - (2) $(h_{(1)} \cdot b)g(h_{(2)}) = g(h_{(1)})(h_{(2)} \cdot b)$ for all $h \in H$ and $b \in B$;
 - (3) $g(hh') = g(h_{(1)})(h_{(2)} \cdot g(h'))$ for all $h, h' \in H$;
 - (4) $g(1) = 1$;
 - (5) g is a coalgebra map; and
 - (6) $\rho(g(h)) = h_{(1)}S(h_{(3)}) \otimes g(h_{(2)})$ for all $h \in H$.
- (b) $\mathcal{N}(B, H)$ is a group under the convolution product.

PROOF: Part (a) follows by Theorem 1, Lemmas 2 and 3, and Corollary 2. Part (b) follows by Corollary 1 and (3.3). It is an interesting exercise to establish part (b) directly from part (a). \square

Observe that if $f \in \text{Aut}_{\mathcal{YD}\text{-Hopf}}(B)$ and $g \in \mathcal{N}(B, H)$ then $f \circ g \in \mathcal{N}(B, H)$ by Proposition 2. The reader is left with the exercise of showing that

$$\varphi : \text{Aut}_{\mathcal{YD}\text{-Hopf}}(B) \rightarrow \text{Aut}_{\text{Group}}(\mathcal{N}(B, H))$$

given by $\varphi(f)(g) = f \circ g$ for $f \in \text{Aut}_{\mathcal{YD}\text{-Hopf}}(A, \pi)$ and $g \in \mathcal{N}(B, H)$ is a well-defined group homomorphism. See Section 4.

Theorem 5. *Let $A = B \times H$ be a biproduct. Then:*

- (a) *There is a one-one group homomorphism*

$$\Phi_{\mathcal{YD}} : \mathcal{N}(B, H)^{op} \rtimes_{\varphi} \text{Aut}_{\mathcal{YD}\text{-Hopf}}(B) \rightarrow \text{Aut}_{\text{Hopf}}(A, \pi)$$

$$\text{given by } \Phi_{\mathcal{YD}}(g, f)(b \times h) = f(b)g(h_{(1)}) \times h_{(2)}.$$

$$(b) \operatorname{Im}(\Phi_{\mathcal{YD}}) = \{F \in \operatorname{Aut}_{\operatorname{Hopf}}(A, \pi) \mid F_L \in \operatorname{Aut}_{\mathcal{YD}-\operatorname{Hopf}}(B)\}.$$

PROOF: To show part (a) let $(g, f), (g', f') \in \mathcal{N}(B, H) \rtimes_{\varphi} \operatorname{Aut}_{\mathcal{YD}-\operatorname{Hopf}}(B)$. That $\Phi_{\mathcal{YD}}(g, f) \in \operatorname{Aut}_{\operatorname{Hopf}}(A, \pi)$ follows by Theorem 1 and Proposition 2. That $\Phi_{\mathcal{YD}}((g, f)(g', f')) = \Phi_{\mathcal{YD}}(g, f) \circ \Phi_{\mathcal{YD}}(g', f')$ follows by Corollary 1. Thus $\Phi_{\mathcal{YD}}$ is a group homomorphism. That $\operatorname{Ker}(\Phi_{\mathcal{YD}})$ is trivial is easy to see. Therefore $\Phi_{\mathcal{YD}}$ is one-one. We have shown part (a).

If $F = \Phi_{\mathcal{YD}}(g, f) \in \operatorname{Im}(\Phi_{\mathcal{YD}})$ then $F_L = f \in \operatorname{Aut}_{\mathcal{YD}-\operatorname{Hopf}}(B)$. Now let $F \in \operatorname{Aut}_{\operatorname{Hopf}}(A, \pi)$ and suppose $F_L \in \operatorname{Aut}_{\mathcal{YD}-\operatorname{Hopf}}(B)$. To establish part (c) we need only show that F_R satisfies the conditions of part (a) of Proposition 2. Since F_L is a coalgebra map part (a)(1) holds for F_R by Corollary 2. Since F_L is a bijective H -module map part (a)(2) holds by virtue of part (e) of Lemma 2. Parts (a)(3) - (a)(6) follow by Lemma 3. We have established part (b). \square

Corollary 6. *Let $A = B \times H$ be a biproduct. If $\operatorname{Im}(\nu) \subseteq \operatorname{Aut}_{\mathcal{YD}-\operatorname{Hopf}}(B)$ then the map $\Phi_{\mathcal{YD}} : \mathcal{N}(B, H)^{op} \rtimes_{\varphi} \operatorname{Aut}_{\mathcal{YD}-\operatorname{Hopf}}(B) \longrightarrow \operatorname{Aut}_{\operatorname{Hopf}}(A, \pi)$ is an isomorphism.* \square

Corollary 7. *Let $A = B \times H$ be a biproduct where B is commutative and H is cocommutative. If F_L is a coalgebra map for all $F \in \operatorname{Aut}_{\operatorname{Hopf}}(A, \pi)$ then the map $\Phi_{\mathcal{YD}} : \mathcal{N}(B, H)^{op} \rtimes_{\varphi} \operatorname{Aut}_{\mathcal{YD}-\operatorname{Hopf}}(B) \longrightarrow \operatorname{Aut}_{\operatorname{Hopf}}(A, \pi)$ is an isomorphism.*

PROOF: Let $F \in \operatorname{Aut}_{\operatorname{Hopf}}(A, \pi)$. Then F_L is a map of left H -modules by part (b) of Corollary 3. If F_L is a coalgebra map then $F_L \in \operatorname{Aut}_{\mathcal{YD}-\operatorname{Hopf}}(B)$ by Lemma 2 and Theorem 1. Now the corollary follows by Corollary 6. \square

In light of Corollary 7, we consider biproducts when H is cocommutative. Suppose H is cocommutative. This is the case, for example, when H is a group algebra. We first revisit Proposition 2. Let $h \in H$ and $g \in \mathcal{N}(B, H)$. Then (a)(6) is $\rho(g(h)) = 1 \otimes g(h)$. Let $b \in B$. In any event

$$g(h)b = g(h_{(1)})(h_{(2)} \cdot (S(h_{(3)}) \cdot b)) = ((h_{(1)}S(h_{(3)})) \cdot b)g(h_{(2)}).$$

Thus $g(h)b = bg(h)$ since H is cocommutative; hence (a)(2) is $\operatorname{Im}(g) \subseteq \mathcal{Z}(B)$. Therefore $\mathcal{N}(B, H) \subseteq \mathcal{Z}(\operatorname{Hom}(H, B))$, where $\operatorname{Hom}(H, B)$ has the convolution algebra structure. In particular $\mathcal{N}(B, H)$ is an abelian group.

Let $F \in \operatorname{Aut}_{\operatorname{Hopf}}(A, \pi)$ and $G \in \operatorname{Ker}(\nu)$. Then $G_R \in \mathcal{Z}(\operatorname{Hom}(H, B))$. We show that $F_L \circ G_R \in \mathcal{N}(B, H)$. Now $F \circ G \circ F^{-1} \in \operatorname{Ker}(\nu)$. Observe that $(F^{-1})_L \circ F_R$ is a left inverse of $(F^{-1})_R$ by part (b) of Corollary 1 and is therefore a right inverse as well by Corollary 5. Using Corollary 1, (3.3),

and the fact that F_L is an algebra map, we compute

$$\begin{aligned}
(F \circ G \circ F^{-1})_R &= ((F \circ G)_L \circ (F^{-1})_R) \star (F \circ G)_R \\
&= ((F_L \circ G_L) \circ (F^{-1})_R) \star ((F_L \circ G_R) \star F_R) \\
&= (F_L \circ (F^{-1})_R) \star ((F_L \circ G_R) \star F_R) \\
&= F_L \circ ((F^{-1})_R \star (G_R \star ((F_L)^{-1} \circ F_R))) \\
&= F_L \circ (G_R \star ((F^{-1})_R \star ((F_L)^{-1} \circ F_R))) \\
&= F_L \circ (G_R \star (\eta \circ \epsilon)) \\
&= F_L \circ G_R.
\end{aligned}$$

Therefore $F_L \circ G_R \in \mathcal{N}(B, H)$. The reader is left with the exercise of showing that

$$\varphi : \text{Im}(\nu) \longrightarrow \text{Aut}_{\text{Group}}(\mathcal{N}(B, H))$$

given by $\varphi(f)(g) = f \circ g$ for $f \in \text{Im}(\nu)$ and $g \in \mathcal{N}(B, H)$ is a well-defined group homomorphism. See Section 4.

Theorem 6. *Let $A = B \times H$ be a biproduct where H is cocommutative. Then:*

- (a) *There is a one-one group homomorphism*

$$\Phi_\nu : \mathcal{N}(B, H)^{\text{op}} \rtimes_\varphi \text{Im}(\nu) \longrightarrow \text{Sym}(A)$$

given by $\Phi_\nu(g, f)(b \times h) = f(b)g(h_{(1)}) \times h_{(2)}$.

- (b) *Let $(g, f) \in \mathcal{N}(B, H)^{\text{op}} \rtimes_\varphi \text{Im}(\nu)$. Then $\Phi_\nu(g, f) \in \text{Aut}_{\text{Hopf}}(A, \pi)$ if and only if $f \in \text{Aut}_{\mathcal{YD}\text{-Hopf}}(B)$.*

PROOF: We first note that $\Phi_\nu(g, f)$ a linear endomorphism of A . Observe that $\Phi_\nu(\eta \circ \epsilon, \text{Id}_B) = \text{Id}_A$ and $\Phi_\nu((g, f)(g', f')) = \Phi_\nu(g, f) \circ \Phi_\nu(g', f')$. Thus $\Phi_\nu(g, f) \in \text{Sym}(A)$ and Φ_ν is a homomorphism.

Suppose $\Phi_\nu(g, f) = \text{Id}_A$. Then $f(b)g(h_{(1)}) \times h_{(2)} = b \times h$ for all $b \in B$ and $h \in H$ from which $(g, f) = (\eta \circ \epsilon, \text{Id}_B)$ follows. Hence Φ_ν is one-one. We have shown part (a).

Suppose $\Phi_\nu(g, f) \in \text{Aut}_{\text{Hopf}}(A, \pi)$. In light of part (c) of Theorem 5, to establish part (b) we need only show that $f \in \text{Aut}_{\mathcal{YD}\text{-Hopf}}(B)$. In light of Lemma 2 and Proposition 2 we need only show that f is a module map. Now $f(h_{(1)} \cdot b)g(h_{(2)}) = g(h_{(1)})(h_{(2)} \cdot f(b))$ for all $h \in H$ and $b \in B$ by part (e) of Lemma 2. Fix b and define $L, R \in \text{Hom}(H, B)$ by $L(h) = f(h \cdot b)$ and $R(h) = h \cdot f(b)$ for all $h \in H$. Then $L \star g = g \star R = R \star g$; the second equation holds since $g \in \mathcal{Z}(\text{Hom}(H, B))$. Now g has a convolution inverse by Corollary 5. Therefore $L = R$ which establishes f is a module map. \square

6. A RELATED BIPRODUCT AND AUTOMORPHISM GROUP

Throughout this section $A = B \times H$ is a biproduct. Here we approach the problem of computing $\text{Im}(\nu)$ of Section 5 by considering a related biproduct.

Let H' be a Hopf subalgebra of H which satisfies $\rho(B) \subseteq H' \otimes B$. Then B is also a left H' -comodule. Regard B as a left H' -module by H -module

action restricted to H' . Then the biproduct $A' = B \times H'$ is defined and A' , regarded as a subspace of A , is a Hopf subalgebra of A . Let $\pi' : A' \rightarrow H'$ be the projection onto H' . Then $\pi' = \pi|_{B \times H'}$.

Now let $F \in \text{Aut}_{\text{Hopf}}(A, \pi)$. Then $F(B \times C) \subseteq B \times C$ for all subcoalgebras C of H by part (c) of Lemma 1; in particular $F(B \times H') \subseteq B \times H'$. Since this inclusion holds for F^{-1} it follows that $F(B \times H') = B \times H'$. Observe that $\pi' \circ (F|_{B \times H'}) = \pi'$ since $\pi \circ F = \pi$. Thus by (3.3) and part (a) of Corollary 1 we have a group homomorphism

$$\Theta : \text{Aut}_{\text{Hopf}}(A, \pi) \rightarrow \text{Aut}_{\text{Hopf}}(A', \pi')$$

defined by $\Theta(F) = F|_{B \times H'}$ for all $F \in \text{Aut}_{\text{Hopf}}(A, \pi)$. By part (a) of Lemma 1 and (3.4) we see

$$(6.1) \quad \Theta(F)_L = F_L \text{ and } \Theta(F)_R = F_R|_{H'}$$

for all $F \in \text{Aut}_{\text{Hopf}}(A, \pi)$. Observe that $\text{Ker}(\Theta)$ corresponds to the set of pairs $(\text{Id}_B, g) \in \mathcal{F}_{B, H}$ such that $g(h) = \epsilon(h)1$ for all $h \in H'$.

Let $\nu' : \text{Aut}_{\text{Hopf}}(A', \pi') \rightarrow \text{Aut}_{\text{Alg}}(A')$ be the group homomorphism defined by $\nu'(F) = F_L$ for all $F \in \text{Aut}_{\text{Hopf}}(A', \pi')$. Then $\nu' \circ \Theta = \nu$, where ν is the map mentioned above. Thus $\text{Im}(\nu) \leq \text{Im}(\nu')$. Which elements of $\text{Im}(\nu')$ belong to $\text{Im}(\nu)$ is easily explained in the context of Theorem 1. Let $f \in \text{Im}(\nu')$. Then $f \in \text{Im}(\nu)$ if and only if there are pairs $(f, g') \in \mathcal{F}_{B, H'}$ and $(f, g) \in \mathcal{F}_{B, H}$ such that $g' = g|_{H'}$.

In biproducts of interest to us below H' is the group algebra of a cyclic group and the left H' -module action on B is trivial.

7. A GENERIC EXAMPLE FROM [9]

Many examples of [9] are described as special cases of [9, Theorem 2]. Our Theorem 7 is [9, Theorem 2] less one technical detail. First a bit of background.

Let V be a vector space and T be an endomorphism of V . For $\lambda \in k$ let $V_\lambda = \{v \in V \mid T(v) = \lambda v\}$. Then T is *diagonalizable* if $V = \sum_{\lambda \in k} V_\lambda$. In any case the sum is direct.

Suppose T is an automorphism and V has a basis B such that $T(B) = B$ and (T) -orbits of B are finite. Then T is diagonalizable if and only if k^\times contains a primitive r^{th} root of unity for every orbit length r . Suppose that T is diagonalizable and has finite order N . Then N is the least common multiple of orbit lengths. Furthermore k^\times has a primitive N^{th} root of unity λ and the cyclic group $U = \langle \lambda \rangle$ is the subgroup of k^\times generated by the set of eigenvalues of T .

If \mathcal{G} is a group and $\theta \in \text{Aut}_{\text{Group}}(\mathcal{G})$ we let $\theta : k[\mathcal{G}] \rightarrow k[\mathcal{G}]$ denote the linear extension of θ to $k[\mathcal{G}]$.

Theorem 7. *Let G and \mathcal{G} be groups, let $\pi : G \rightarrow \text{Aut}_{\text{Group}}(\mathcal{G})$ be a group homomorphism, and let $\theta \in \text{Aut}_{\text{Group}}(\mathcal{G})$. Suppose that the (θ) -orbits of \mathcal{G} are finite and that θ is diagonalizable. Assume further that:*

- (a) $\pi(g) \circ \theta = \theta \circ \pi(g)$ for all $g \in G$.
- (b) There exists an isomorphism $U \longrightarrow \mathbf{U}$ ($\lambda \mapsto \boldsymbol{\lambda}$) of the subgroup $U \subseteq k^\times$ generated by the eigenvalues of θ and a subgroup \mathbf{U} of G which satisfies $\mathbf{U} \subseteq \text{Ker}(\pi) \cap Z(G)$.

Let $H = k[G]$ and $B = k[\mathcal{G}]$ Then:

- (c) B is a left H -module determined by $g \cdot b = \pi(g)(b)$ for all $g \in G$ and $b \in \mathcal{G}$.
- (d) B is a left H -comodule where $\rho(b) = \boldsymbol{\lambda} \otimes b$ for $b \in B_\lambda$.
- (e) The biproduct $A = B \times H$ is defined for the Hopf algebra B with these module and comodule structures. Furthermore A is a cosemisimple involutory Hopf algebra over k .

□

About the preceding theorem. Observe that $\rho(B) \subseteq k[\mathbf{U}]$. Our discussion of Section 6 applies to $H' = k[\mathbf{U}]$. Note that \mathbf{U} is a cyclic group and that the left H' -module action on B is trivial. A group of great interest to us is $\text{Aut}_{\text{Hopf}}(A', \pi')$.

To continue our discussion of Theorem 7. We emphasize that $B = k[\mathcal{G}]$ is a Hopf algebra over k whose coproduct also satisfies (1.4). Note that a map $f: B \longrightarrow B$ is a map of left H -comodules if and only if $f(B_\lambda) \subseteq B_\lambda$ for all $\lambda \in k$; that is if and only if $\theta \circ f = f \circ \theta$.

In many cases $\text{Im}(\pi) \subseteq (\theta)$, for example when the left H -module action on B is trivial. Suppose $\text{Im}(\pi) \subseteq (\theta)$. If f is a map of left H -comodules then f is a map of left H -modules as well. We revisit Theorem 1 in the next corollary. Its proof is left to the reader:

Corollary 8. *Let $A = B \times H$ be the biproduct described in Theorem 7 and further assume that $\text{Im}(\pi) \subseteq (\theta)$. Then $(f, g) \in \mathcal{F}_{B, H}^\bullet$ if and only if:*

$f: B \longrightarrow B$ is an algebra automorphism such that

- (a) $\epsilon \circ f = \epsilon$,
- (b) $\Delta f(b) = f(b_{(1)})g(b_{(2)(-1)}) \otimes f(b_{(2)(0)})$ for all $b \in B$,
- (c) $\theta \circ f = f \circ \theta$; and

$g: H \longrightarrow B$ is a Hopf algebra map such that

- (d) $\text{Im}(g) \subseteq Z(B)$ and
- (e) $\theta \circ g = g$.

□

When \mathcal{G} is abelian (d) is redundant. We consider the case when \mathcal{G} is abelian in the next section. In this situation:

Corollary 9. *Let $A = B \times H$ be the biproduct described in Theorem 7. Suppose that $\text{Im}(\pi) \subseteq (\theta)$ and \mathcal{G} is abelian. Then $\mathcal{N}(B, H)$ consists of the Hopf algebra maps $g: H \longrightarrow B$ which satisfy $\theta \circ g = g$ and $g(\mathbf{U}) = \{1\}$. □*

8. THE SPECIAL CASE $A' = k[\mathcal{G}] \times k[\mathbf{U}]$ WHEN \mathcal{G} IS FINITE ABELIAN

Let \mathcal{G} be a finite abelian group of order n , suppose k has a primitive n^{th} root of unity ω , and let $A = k[\mathcal{G}] \times H$ be the biproduct of Theorem 7. Then $B = k[\mathcal{G}]$ is commutative and H is cocommutative. The map $\Phi_{\mathcal{YD}}$ of Corollary 7 is a group isomorphism if and only if F_L is a coalgebra map for all $F \in \text{Aut}_{\text{Hopf}}(A, \pi)$. We are interested in when $\Phi_{\mathcal{YD}}$ is an isomorphism. In light of (6.1) we are led to consider the special case $A' = k[\mathcal{G}] \times k[\mathbf{U}]$ of the biproduct described in the preceding section. Recall that the $k[\mathbf{U}]$ -module action on B is trivial. Corollary 8 applies to A' .

In this section we study A' . We describe the group $\text{Aut}_{\text{Hopf}}(A', \pi')$ in terms permutations and characters in Theorem 8. Our discussion is based on the orthogonal basis of idempotents for $B = k[\mathcal{G}]$.

Write $\mathcal{G} = \mathcal{G}_1 \times \cdots \times \mathcal{G}_t$ as a product of cyclic groups, where $\mathcal{G}_j = \langle g_j \rangle$ and has order n_j for all $1 \leq j \leq t$. Then $n = n_1 \cdots n_t$ and $\omega_j = \omega^{n/n_j}$ is a primitive n_j^{th} root of unity each $1 \leq j \leq t$. Let $\mathbf{G} = \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_t}$ with its usual *ring* structure. For $\mathbf{m} = (m_1, \dots, m_t) \in \mathbf{G}$ we define formal powers

$$g^{(\mathbf{m})} = (g_1^{m_1}, \dots, g_t^{m_t}) \quad \text{and} \quad \omega^{(\mathbf{m})} = \omega_1^{m_1} \cdots \omega_t^{m_t}.$$

The maps $\mathbf{G} \rightarrow \mathcal{G}$ and $\mathbf{G} \rightarrow k^\times$ defined by $\mathbf{m} \mapsto g^{(\mathbf{m})}$ and $\mathbf{m} \mapsto \omega^{(\mathbf{m})}$ respectively are group homomorphisms, the first is an isomorphism. Set

$$(8.1) \quad e_{\mathbf{m}} = \sum_{\mathbf{r} \in \mathbf{G}} (\omega^{(\mathbf{m}\mathbf{r})}/n) g^{(\mathbf{r})}$$

for all $\mathbf{m} \in \mathbf{G}$. Then $\{e_{\mathbf{m}}\}_{\mathbf{m} \in \mathbf{G}}$ is a linear basis for B which satisfies

$$(8.2) \quad \sum_{\mathbf{m} \in \mathbf{G}} e_{\mathbf{m}} = 1 \quad \text{and} \quad e_{\mathbf{m}} e_{\mathbf{n}} = \delta_{\mathbf{m}, \mathbf{n}} e_{\mathbf{n}}$$

for all $\mathbf{m}, \mathbf{n} \in \mathbf{G}$. Since $\{e_{\mathbf{m}}\}_{\mathbf{m} \in \mathbf{G}}$ is a linear basis for $B = k[\mathcal{G}]$ the algebra structure of B is determined by (8.2). Observe that

$$(8.3) \quad g^{(\mathbf{m})} e_{\mathbf{n}} = \omega^{(-\mathbf{m}\mathbf{n})} e_{\mathbf{n}}$$

for all $\mathbf{m}, \mathbf{n} \in \mathbf{G}$. Let $\mathbf{m} \in \mathbf{G}$. The map $\alpha_{\mathbf{m}} : \mathbf{G} \rightarrow k^\times$ defined by $\alpha_{\mathbf{m}}(\mathbf{n}) = \omega^{(-\mathbf{m}\mathbf{n})}$ for all $\mathbf{n} \in \mathbf{G}$ belongs to the character group $\widehat{\mathbf{G}} = \text{Char}(\mathbf{G}, k^\times)$. Note

$$(8.4) \quad g^{(\mathbf{m})} = \sum_{\mathbf{n} \in \mathbf{G}} \alpha_{\mathbf{m}}(\mathbf{n}) e_{\mathbf{n}}$$

by (8.2) and (8.3). Therefore the group homomorphism $\mathbf{G} \rightarrow \widehat{\mathbf{G}}$ defined by $\mathbf{m} \mapsto \alpha_{\mathbf{m}}$ is one-one and consequently is an isomorphism.

The coalgebra structure of B in terms of this basis is given by

$$(8.5) \quad \Delta(e_{\mathbf{m}}) = \sum_{\mathbf{j} \in \mathbf{G}} e_{\mathbf{j}} \otimes e_{\mathbf{m}-\mathbf{j}} \quad \text{and} \quad \epsilon(e_{\mathbf{m}}) = \delta_{\mathbf{m}, \mathbf{0}}$$

for all $\mathbf{m} \in \mathbf{G}$, where $\mathbf{0}$ is the neutral element for the additive group structure of \mathbf{G} . Note that the unique integral Λ for the Hopf algebra B which satisfies $\epsilon(\Lambda) = 1$ is $\Lambda = e_{\mathbf{0}}$.

For $\tau \in \text{Sym}(\mathbf{G})$ let F_τ be the linear automorphism of B defined by $F_\tau(e_{\mathbf{m}}) = e_{\tau(\mathbf{m})}$ for all $\mathbf{m} \in \mathbf{G}$.

Lemma 4. *The correspondence $\tau \mapsto F_\tau$ describes a group isomorphism $\text{Sym}(\mathbf{G}) \simeq \text{Aut}_{\text{Alg}}(B)$ which restricts to an isomorphism $\text{Aut}_{\text{Group}}(\mathbf{G}) \simeq \text{Aut}_{\text{Hopf}}(B)$.*

PROOF: Let $\tau, \sigma \in \text{Sym}(\mathbf{G})$. Then $F_\sigma \circ F_\tau = F_{\sigma \circ \tau}$. It is easy to see that $F_\tau \in \text{Aut}_{\text{Alg}}(B)$ and that the map $\tau \mapsto F_\tau$ is one-one. Let $f \in \text{Aut}_{\text{Alg}}(B)$. We will show that $f = F_\tau$ for some $\tau \in \text{Sym}(\mathbf{G})$.

The $ke_{\mathbf{m}}$'s are the minimal ideals of $k[\mathcal{G}]$ and f is an automorphism. Thus f permutes the $ke_{\mathbf{m}}$'s. Therefore there is a $\tau \in \text{Sym}(\mathbf{G})$ such that $f(ke_{\mathbf{m}}) = ke_{\tau(\mathbf{m})}$ for all $\mathbf{m} \in \mathbf{G}$. Let $\mathbf{m} \in \mathbf{G}$. Since $f(e_{\mathbf{m}})$ is a non-zero idempotent $f(e_{\mathbf{m}}) = e_{\tau(\mathbf{m})}$. We have shown $f = F_\tau$ which establishes the first isomorphism.

As for the second, let $\tau \in \text{Sym}(\mathbf{G})$. It is easy to see that $\epsilon \circ F_\tau = \epsilon$ if and only if $\tau(\mathbf{0}) = \mathbf{0}$. Let $\mathbf{m} \in \mathbf{G}$. Then

$$\Delta(F_\tau(e_{\mathbf{m}})) = \Delta(e_{\tau(\mathbf{m})}) = \sum_{\mathbf{r} \in \mathbf{G}} e_{\mathbf{r}} \otimes e_{\tau(\mathbf{m}) - \mathbf{r}} = \sum_{\mathbf{r} \in \mathbf{G}} e_{\tau(\mathbf{r})} \otimes e_{\tau(\mathbf{m}) - \tau(\mathbf{r})}$$

and

$$(F_\tau \otimes F_\tau)(\Delta(e_{\mathbf{m}})) = \sum_{\mathbf{r} \in \mathbf{G}} F_\tau(e_{\mathbf{r}}) \otimes F_\tau(e_{\mathbf{m} - \mathbf{r}}) = \sum_{\mathbf{r} \in \mathbf{G}} e_{\tau(\mathbf{r})} \otimes e_{\tau(\mathbf{m} - \mathbf{r})}.$$

Therefore $\Delta \circ F_\tau = (F_\tau \otimes F_\tau) \circ \Delta$ if and only if $\tau(\mathbf{m}) - \tau(\mathbf{r}) = \tau(\mathbf{m} - \mathbf{r})$ for all $\mathbf{m}, \mathbf{r} \in \mathbf{G}$. We have shown that F_τ is a coalgebra map if and only if $\tau(\mathbf{0}) = \mathbf{0}$ and this last condition holds which is equivalent to saying $\tau \in \text{Aut}_{\text{Group}}(\mathbf{G})$. We have established the second isomorphism. \square

We turn our attention to $A' = k[\mathcal{G}] \times k[\mathbf{U}]$. Let $F \in \text{Aut}_{\text{Hopf}}(A', \pi')$ and $(f, g) \in \mathcal{F}_{k[\mathcal{G}], k[\mathbf{U}]}^\bullet$ correspond to it according to Theorem 1. First of all

$$(8.6) \quad \theta = F_\sigma \text{ and } f = F_\tau$$

for unique $\sigma \in \text{Aut}_{\text{Group}}(\mathbf{G})$ and $\tau \in \text{Sym}(\mathbf{G})$ by Lemma 4. Since $\epsilon \circ f = \epsilon$ by part (a) of Corollary 8, by the second equation of (8.5) it follows that

$$(8.7) \quad \tau(\mathbf{0}) = \mathbf{0}.$$

By part (c) of Corollary 8 we have $F_\sigma \circ F_\tau = F_\tau \circ F_\sigma$ and therefore

$$(8.8) \quad \sigma \circ \tau = \tau \circ \sigma.$$

Further analysis of $f = F_\tau$ is done in terms of the (θ) -orbits of $k[\mathcal{G}]$. We continue with the notation of Theorem 7 and draw from the discussion preceding it in Section 7.

Let N be the order of θ , which is also the order of θ . Then N is the least common multiple of the (θ) -orbit lengths of $k[\mathcal{G}]$, which is also the least

common multiple of the lengths of the (θ) -orbit of \mathcal{G} . The eigenvalues of θ generate a (cyclic) subgroup U of k^\times of order N . Choose a generator λ for U and let $\lambda \in \mathbf{U}$ be its counterpart. Then λ is a primitive N^{th} root of unity, λ has order N , and $\mathbf{U} = (\lambda)$.

Let $b \in B$. Denote the (θ) -orbit of b by $\mathcal{O}_{\theta,b}$ and set $r = |\mathcal{O}_{\theta,b}|$. Then $\mathcal{O}_{\theta,b} = \{b, \theta(b), \dots, \theta^{r-1}(b)\}$, where $\theta^r(b) = b$, and r divides $|\theta| = |\mathbf{U}| = N$. In particular $\lambda_r = \lambda^{N/r}$ is a primitive r^{th} root of unity.

For $0 \leq i \leq r-1$ define $b_{\lambda_r^i} = \sum_{\ell=0}^{r-1} (\lambda_r^{-i\ell}/r) \theta^\ell(b)$. It is an easy exercise to see that $\theta(b_{\lambda_r^i}) = \lambda_r^i b_{\lambda_r^i}$ and that $\theta^i(b) = \sum_{\ell=0}^{r-1} \lambda_r^{i\ell} b_{\lambda_r^\ell}$ for all $0 \leq i \leq r-1$. In particular the linear span $\text{sp}(\mathcal{O}_{\theta,b})$ of $\mathcal{O}_{\theta,b}$ has a basis of eigenvectors belonging to distinct eigenvalues of θ and these constitute the r^{th} roots of unity of k^\times .

Let $\mathbf{m} \in \mathbf{G}$. We specialize our discussion and notation for $b = e_{\mathbf{m}}$. We write $\mathcal{O}_{\theta,\mathbf{m}}$ for $\mathcal{O}_{\theta,e_{\mathbf{m}}}$, $|\mathbf{m}|$ for r , $\lambda_{\mathbf{m}}$ for λ_r , and $e_{\mathbf{m},\lambda_{\mathbf{m}}^i}$ for $b_{\lambda_r^i}$. Let $\lambda_{\mathbf{m}} \in \mathbf{U}$ be the counterpart of $\lambda_{\mathbf{m}} \in k^\times$. Then $\lambda_{\mathbf{m}} = \lambda^{N/|\mathbf{m}|}$,

$$(8.9) \quad \mathcal{O}_{\theta,\mathbf{m}} = \{e_{\mathbf{m}}, e_{\sigma(\mathbf{m})}, \dots, e_{\sigma^{|\mathbf{m}|-1}(\mathbf{m})}\}, \text{ where } \sigma^{|\mathbf{m}|}(\mathbf{m}) = \mathbf{m},$$

$$(8.10) \quad e_{\mathbf{m},\lambda_{\mathbf{m}}^i} = \sum_{\ell \in \mathbb{Z}_{|\mathbf{m}|}} (\lambda_{\mathbf{m}}^{-i\ell}/|\mathbf{m}|) e_{\sigma^\ell(\mathbf{m})},$$

and

$$(8.11) \quad e_{\sigma^i(\mathbf{m})} = \sum_{\ell \in \mathbb{Z}_{|\mathbf{m}|}} \lambda_{\mathbf{m}}^{i\ell} e_{\mathbf{m},\lambda_{\mathbf{m}}^\ell}$$

for all $0 \leq i \leq |\mathbf{m}|-1$. Now $\mathcal{O}_{\theta,b} = \mathcal{O}_{\theta,\theta(b)}$; thus $|\mathbf{m}| = |\sigma(\mathbf{m})|$. Consequently

$$(8.12) \quad \lambda_{\mathbf{m}} = \lambda_{\sigma(\mathbf{m})} \text{ and } \lambda_{\mathbf{m}} = \lambda_{\sigma(\mathbf{m})}.$$

Let $\mathbf{s} \in \mathbf{G}$ and $c = e_{\mathbf{s}}$. We find necessary and sufficient conditions for part (b) of Corollary 8 to hold for c ; that is

$$(8.13) \quad \Delta(f(c)) = f(c_{(1)})g(c_{(2)(-1)}) \otimes f(c_{(2)(0)}).$$

First of all

$$\begin{aligned} c_{(1)} \otimes c_{(2)(-1)} \otimes c_{(2)(0)} &= \sum_{\mathbf{m} \in \mathbf{G}} e_{\mathbf{s}-\mathbf{m}} \otimes \rho(e_{\mathbf{m}}) \\ &= \sum_{\mathbf{m} \in \mathbf{G}} e_{\mathbf{s}-\mathbf{m}} \otimes \rho\left(\sum_{i \in \mathbb{Z}_{|\mathbf{m}|}} e_{\mathbf{m},\lambda_{\mathbf{m}}^i}\right) \\ &= \sum_{\mathbf{m} \in \mathbf{G}} \sum_{i \in \mathbb{Z}_{|\mathbf{m}|}} e_{\mathbf{s}-\mathbf{m}} \otimes \lambda_{\mathbf{m}}^i \otimes e_{\mathbf{m},\lambda_{\mathbf{m}}^i} \\ &= \sum_{\mathbf{m} \in \mathbf{G}} \sum_{i, \ell \in \mathbb{Z}_{|\mathbf{m}|}} e_{\mathbf{s}-\mathbf{m}} \otimes \lambda_{\mathbf{m}}^i \otimes (\lambda_{\mathbf{m}}^{-i\ell}/|\mathbf{m}|) e_{\sigma^\ell(\mathbf{m})}. \end{aligned}$$

We interrupt our calculation to organize several technicalities.

Lemma 5. *Let $A' = k[\mathcal{G}] \times k[\mathbf{U}]$ be the biproduct described above and suppose $(f, g) \in \mathcal{F}_{k[\mathcal{G}], k[\mathbf{U}]}^\bullet$. Then:*

- (a) $f^{-1} \circ g : k[\mathbf{U}] \longrightarrow k[\mathcal{G}]$ is a Hopf algebra map and $\theta \circ (f^{-1} \circ g) = f^{-1} \circ g$.
- (b) Let $g_\lambda = (f^{-1} \circ g)(\lambda)$. Then $g_\lambda \in \mathcal{G}$, $\theta(g_\lambda) = g_\lambda$, $g_\lambda^N = 1$, and $g_\lambda^{N/|\mathbf{m}|} = (f^{-1} \circ g)(\lambda_{\mathbf{m}})$ for all $\mathbf{m} \in \mathbf{G}$.
- (c) There exists $\alpha \in \widehat{\mathbf{G}}$ which is determined by $g_\lambda e_{\mathbf{s}} = \alpha(\mathbf{s}) e_{\mathbf{s}}$ for all $\mathbf{s} \in \mathbf{G}$. Furthermore $g_\lambda^\ell e_{\mathbf{s}} = \alpha(\mathbf{s})^\ell e_{\mathbf{s}}$ for all $\ell \in \mathbb{Z}$, $\mathbf{s} \in \mathbf{G}$, $\alpha \circ \sigma = \alpha$, and $\alpha(\mathbf{s})^N = 1$ for all $\mathbf{s} \in \mathbf{G}$.
- (d) For all $\mathbf{s}, \mathbf{m} \in \mathbf{G}$ there exists an integer $\ell(\mathbf{s}, \mathbf{m})$ which is determined by $0 \leq \ell(\mathbf{s}, \mathbf{m}) < |\mathbf{m}|$ and $(\alpha(\mathbf{s})/\alpha(\mathbf{m}))^{N/|\mathbf{m}|} = \lambda_{\mathbf{m}}^{\ell(\mathbf{s}, \mathbf{m})}$.
- (e) $\ell(\sigma(\mathbf{s}), \mathbf{m}) = \ell(\mathbf{s}, \mathbf{m}) = \ell(\mathbf{s}, \sigma(\mathbf{m}))$ for all $\mathbf{s}, \mathbf{m} \in \mathbf{G}$.

PROOF: To show part (a) we first note by Corollary 8 that $g : k[\mathbf{U}] \longrightarrow k[\mathcal{G}]$ is a Hopf algebra map which satisfies $\theta \circ g = g$ and $f : k[\mathcal{G}] \longrightarrow k[\mathcal{G}]$ is an algebra automorphism which satisfies $\theta \circ f = f \circ \theta$ and $\epsilon \circ f = \epsilon$. Thus $f^{-1} \circ g$ is an algebra map which satisfies $\theta \circ (f^{-1} \circ g) = f^{-1} \circ g$ and $\epsilon \circ (f^{-1} \circ g) = \epsilon$.

Let $h \in k[\mathbf{U}]$. The condition $\theta \circ g = g$ implies $\rho(g(h)) = 1 \otimes g(h)$; thus

$$g(h)_{(1)} \otimes g(h)_{(2)(-1)} \otimes g(h)_{(2)(0)} = g(h)_{(1)} \otimes 1 \otimes g(h)_{(2)}$$

since g is a coalgebra map. Since (f, g) corresponds to an automorphism, $(f^{-1}, g') \in \mathcal{F}_{k[\mathcal{G}], k[\mathbf{U}]}^\bullet$ for some g' by (3.3), part (a) of Corollary 1, and Theorem 1. Now we apply part (b) of Corollary 8 to the pair (f^{-1}, g') to conclude that $f^{-1} \circ g$ is a coalgebra map. This concludes the proof of part (a).

Note that $g_\lambda \in G(k[\mathcal{G}]) = \mathcal{G}$ since $\lambda \in \mathbf{U} = G(k[\mathbf{U}])$ and $f^{-1} \circ g$ is a coalgebra map. The remainder of part (b) easily follows by part (a). As for part (c), the existence of α follows from the bijection $\mathbf{G} \longrightarrow \widehat{\mathbf{G}}$ described just after (8.2). Now $\theta(g_\lambda) = g_\lambda$ by part (b). The calculation

$$g_\lambda e_{\sigma(\mathbf{s})} = \theta(g_\lambda e_{\mathbf{s}}) = \theta(\alpha(\mathbf{s}) e_{\mathbf{s}}) = \alpha(\mathbf{s}) e_{\sigma(\mathbf{s})}$$

for all $\mathbf{s} \in \mathbf{G}$ shows that $\alpha = \alpha \circ \sigma^{-1}$, or equivalently

$$(8.14) \quad \alpha \circ \sigma = \alpha.$$

Since $g_\lambda^N = 1$ the remainder of the proof of part (c) easily follows.

To show part (d), we recall $\alpha(\mathbf{n})^N = 1$ for all $\mathbf{n} \in \mathbf{G}$ by part (c). Let $\mathbf{s}, \mathbf{m} \in \mathbf{G}$. Then $(\alpha(\mathbf{s})/\alpha(\mathbf{m}))^{N/|\mathbf{m}|}$ is an $|\mathbf{m}|^{th}$ root of unity. Since $\lambda_{\mathbf{m}} = \lambda^{N/|\mathbf{m}|}$ is a primitive $|\mathbf{m}|^{th}$ root of unity, there exists a unique solution to $(\alpha(\mathbf{s})/\alpha(\mathbf{m}))^{N/|\mathbf{m}|} = \lambda_{\mathbf{m}}^\ell$ where $0 \leq \ell < |\mathbf{m}|$. We have shown that part (d) holds. Part (e) follows from part (d), (8.12), and the fact that $\alpha \circ \sigma = \alpha$. \square

Using the preceding lemma we calculate

$$\begin{aligned}
& f(c_{(1)})g(c_{(2)(-1)}) \otimes f(c_{(2)(0)}) \\
&= \sum_{\mathbf{m} \in \mathbf{G}} \sum_{i, \ell \in \mathbb{Z}_{|\mathbf{m}|}} f(e_{\mathbf{s}-\mathbf{m}})g(\lambda_{\mathbf{m}}^i) \otimes (\lambda_{\mathbf{m}}^{-i\ell}/|\mathbf{m}|)f(e_{\sigma^\ell(\mathbf{m})}) \\
&= \sum_{\mathbf{m} \in \mathbf{G}} \sum_{i, \ell \in \mathbb{Z}_{|\mathbf{m}|}} f(e_{\mathbf{s}-\mathbf{m}}((f^{-1} \circ g)(\lambda_{\mathbf{m}}))^i) \otimes (\lambda_{\mathbf{m}}^{-i\ell}/|\mathbf{m}|)f(e_{\sigma^\ell(\mathbf{m})}) \\
&= \sum_{\mathbf{m} \in \mathbf{G}} \sum_{i, \ell \in \mathbb{Z}_{|\mathbf{m}|}} f(e_{\mathbf{s}-\mathbf{m}}\alpha(\mathbf{s}-\mathbf{m})^{(N/|\mathbf{m}|)i}) \otimes (\lambda_{\mathbf{m}}^{-i\ell}/|\mathbf{m}|)f(e_{\sigma^\ell(\mathbf{m})}) \\
&= \sum_{\mathbf{m} \in \mathbf{G}} \sum_{i, \ell \in \mathbb{Z}_{|\mathbf{m}|}} \alpha(\mathbf{s}-\mathbf{m})^{(N/|\mathbf{m}|)i} (\lambda_{\mathbf{m}}^{-i\ell}/|\mathbf{m}|) e_{\tau(\mathbf{s}-\mathbf{m})} \otimes e_{\tau(\sigma^\ell(\mathbf{m}))} \\
&= \sum_{\mathbf{m} \in \mathbf{G}} \sum_{i, \ell \in \mathbb{Z}_{|\mathbf{m}|}} (\lambda_{\mathbf{m}}^{(\ell(\mathbf{s}, \mathbf{m})-\ell)i}/|\mathbf{m}|) e_{\tau(\mathbf{s}-\mathbf{m})} \otimes e_{\tau(\sigma^\ell(\mathbf{m}))} \\
&= \sum_{\mathbf{m} \in \mathbf{G}} e_{\tau(\mathbf{s}-\mathbf{m})} \otimes e_{\tau(\sigma^{\ell(\mathbf{s}, \mathbf{m})}(\mathbf{m}))}.
\end{aligned}$$

On the other hand

$$\Delta(f(c)) = \Delta(e_{\tau(\mathbf{s})}) = \sum_{\mathbf{m} \in \mathbf{G}} e_{\tau(\mathbf{s})-\mathbf{m}} \otimes e_{\mathbf{m}} = \sum_{\mathbf{m} \in \mathbf{G}} e_{\tau(\mathbf{s})-\tau(\mathbf{m})} \otimes e_{\tau(\mathbf{m})}.$$

Therefore (8.13) holds if and only if

$$(8.15) \quad \sum_{\mathbf{m} \in \mathbf{G}} e_{\tau(\mathbf{s})-\tau(\mathbf{m})} \otimes e_{\tau(\mathbf{m})} = \sum_{\mathbf{m} \in \mathbf{G}} e_{\tau(\mathbf{s}-\mathbf{m})} \otimes e_{\tau(\sigma^{\ell(\mathbf{s}, \mathbf{m})}(\mathbf{m}))}.$$

Note that (8.15) holds if and only if it holds when the index of summation runs over a (θ) -orbit of \mathbf{G} for all orbits.

Let $\mathbf{m} \in \mathbf{G}$ and $\mathcal{O} = \mathcal{O}_{\theta, \mathbf{m}}$. Since $\sigma^{\ell(\mathbf{s}, \mathbf{m})}$ permutes \mathcal{O} , and $\ell(\mathbf{s}, \mathbf{n}) = \ell(\mathbf{s}, \mathbf{m})$ for all $\mathbf{n} \in \mathcal{O}$ by part (e) of Lemma 5, the equation of (8.15) when the index of summation runs over \mathcal{O} can be written

$$(8.16) \quad \sum_{\mathbf{n} \in \mathcal{O}} e_{\tau(\mathbf{s})-\tau(\sigma^{\ell(\mathbf{s}, \mathbf{m})}(\mathbf{n}))} \otimes e_{\tau(\sigma^{\ell(\mathbf{s}, \mathbf{m})}(\mathbf{n}))} = \sum_{\mathbf{n} \in \mathcal{O}} e_{\tau(\mathbf{s}-\mathbf{n})} \otimes e_{\tau(\sigma^{\ell(\mathbf{s}, \mathbf{m})}(\mathbf{n}))}.$$

Therefore part (b) of Corollary 8 holds for all $b \in k[\mathcal{G}]$ if and only if

$$(8.17) \quad \tau(\mathbf{s}-\mathbf{m}) = \tau(\mathbf{s}) - \tau(\sigma^{\ell(\mathbf{s}, \mathbf{m})}(\mathbf{m}))$$

for all $\mathbf{s}, \mathbf{m} \in \mathbf{G}$.

We are now in a position to characterize the elements of $\text{Aut}_{\text{Hopf}}(A', \pi')$, or equivalently the elements of $\mathcal{F}_{k[\mathcal{G}], k[\mathbf{U}]}^\bullet$, in terms of certain elements of $\text{Sym}(\mathbf{G})$ and $\widehat{\mathbf{G}}$. For $\mathbf{m} \in \mathbf{G}$ observe that $|\mathbf{m}|$ is also the length of the (σ) -orbit of \mathbf{m} . See (8.9).

Let \mathbf{G} be any finite abelian group and $\sigma \in \text{Aut}_{\text{Group}}(\mathbf{G})$. Suppose k^\times contain a primitive $|\sigma|^{th}$ root of unity λ . Let $\mathcal{F}_{\mathbf{G}, \sigma, \lambda}$ be the set of all pairs (τ, α) , where $\tau \in \text{Sym}(\mathbf{G})$ and $\alpha \in \widehat{\mathbf{G}}$, such that:

- (F.a) $\tau \circ \sigma = \sigma \circ \tau$;
- (F.b) $\alpha \circ \sigma = \alpha$;
- (F.c) $\alpha^N = 1$, where N is the order of σ ; and
- (F.d) $\tau(\mathbf{s} - \mathbf{m}) = \tau(\mathbf{s}) - \tau(\sigma^{\ell_\alpha(\mathbf{s}, \mathbf{m})}(\mathbf{m}))$ for all $\mathbf{s}, \mathbf{m} \in \mathbf{G}$, where $\ell_\alpha(\mathbf{s}, \mathbf{m})$ is the integer determined by the conditions $0 \leq \ell_\alpha(\mathbf{s}, \mathbf{m}) < |\mathbf{m}|$ and $(\alpha(\mathbf{s})/\alpha(\mathbf{m}))^{N/|\mathbf{m}|} = \lambda_{\mathbf{m}}^{\ell_\alpha(\mathbf{s}, \mathbf{m})}$.

Observe that if $\beta \in \widehat{\mathbf{G}}$ and satisfies $\beta \circ \sigma = \beta$ then $\beta \circ \tau \in \widehat{\mathbf{G}}$ by (F.b) and (F.e). If $(\tau, \alpha) \in \mathcal{F}_{\mathbf{G}, \sigma, \lambda}$ then

$$(F.e) \quad \ell_\alpha(\sigma(\mathbf{s}), \mathbf{m}) = \ell_\alpha(\mathbf{s}, \mathbf{m}) = \ell_\alpha(\mathbf{s}, \sigma(\mathbf{m}))$$

for all $\mathbf{s}, \mathbf{m} \in \mathbf{G}$ for all $\mathbf{s}, \mathbf{m} \in \mathbf{G}$ since $\alpha \circ \sigma = \alpha$ and $|\sigma(\mathbf{m})| = |\mathbf{m}|$ for all $\mathbf{m} \in \mathbf{G}$.

Theorem 8. *Let $A' = k[\mathcal{G}] \times k[\mathbf{U}]$ be the biproduct described above, where $\mathbf{U} = (\boldsymbol{\lambda})$, $\boldsymbol{\theta} = F_\sigma$, and $\lambda \in k^\times$ is a primitive $|\sigma|^{th}$ root of unity. Then:*

- (a) *There is a bijection $\mathcal{F}_{k[\mathcal{G}], k[\mathbf{U}]}^\bullet \longrightarrow \mathcal{F}_{\mathbf{G}, \sigma, \lambda}$ given by $(f, g) \mapsto (\tau, \alpha)$, where $f = F_\tau$ and α is determined by $g(\boldsymbol{\lambda})e_{\tau(\mathbf{s})} = \alpha(\mathbf{s})e_{\tau(\mathbf{s})}$ for all $\mathbf{s} \in \mathbf{G}$.*
- (b) *With the identification of $\mathcal{F}_{\mathbf{G}, \sigma, \lambda}$ and $\mathcal{F}_{k[\mathcal{G}], k[\mathbf{U}]}^\bullet$ via the bijection of part (a), the element $F \in \text{Aut}_{\text{Hopf}}(A', \pi')$ corresponding to (τ, α) as in part (a) of Theorem 1 is determined by*

$$F(e_{\mathbf{s}} \times \boldsymbol{\lambda}^\ell) = \alpha(\mathbf{s})^\ell e_{\tau(\mathbf{s})} \times \boldsymbol{\lambda}^\ell$$

for all $\mathbf{s} \in \mathbf{G}$ and $0 \leq \ell < |\mathbf{U}|$.

PROOF: Let $(f, g) \in \mathcal{F}_{k[\mathcal{G}], k[\mathbf{U}]}^\bullet$. Then $f = F_\tau$ for a unique $\tau \in \text{Sym}(\mathbf{G})$ by (8.6). Let $g_\lambda = (f^{-1} \circ g)(\boldsymbol{\lambda})$. There exists $\alpha \in \widehat{\mathbf{G}}$ such that $g_\lambda e_{\mathbf{s}} = \alpha(\mathbf{s})e_{\mathbf{s}}$ for all $\mathbf{s} \in \mathbf{G}$ by part (c) of Lemma 5. Since f is an algebra map $f(g_\lambda)f(e_{\mathbf{s}}) = f(g_\lambda e_{\mathbf{s}}) = \alpha(\mathbf{s})f(e_{\mathbf{s}})$ for all $\mathbf{s} \in \mathbf{G}$. Thus $g(\boldsymbol{\lambda})e_{\tau(\mathbf{s})} = \alpha(\mathbf{s})e_{\tau(\mathbf{s})}$ for all $\mathbf{s} \in \mathbf{G}$. The preceding equation determines α . That $(\tau, \alpha) \in \mathcal{F}_{\mathbf{G}, \sigma, \lambda}$ follows by (8.8), (8.14), parts (c)–(e) of Lemma 5, and (8.17). The association $(f, g) \mapsto (\tau, \alpha)$ defines a function $\mathbf{f} : \mathcal{F}_{k[\mathcal{G}], k[\mathbf{U}]}^\bullet \longrightarrow \mathcal{F}_{\mathbf{G}, \sigma, \lambda}$.

Now let $(\tau, \alpha) \in \mathcal{F}_{\mathbf{G}, \sigma, \lambda}$. Then $f = F_\tau$ is an algebra automorphism of $k[\mathcal{G}]$ by Lemma 4. Let $\mathbf{g} \in k[\mathcal{G}]$ be defined by $\mathbf{g}e_{\mathbf{s}} = \alpha(\mathbf{s})e_{\mathbf{s}}$ for all $\mathbf{s} \in \mathbf{G}$. Then $\mathbf{g} \in \mathcal{G}$; see (8.4) and the subsequent remark. Since f is an algebra map $f(\mathbf{g})e_{\tau(\mathbf{s})} = \alpha(\mathbf{s})e_{\tau(\mathbf{s})}$, or equivalently $f(\mathbf{g})e_{\mathbf{s}} = (\alpha \circ \tau^{-1})(\mathbf{s})e_{\mathbf{s}}$, for all $\mathbf{s} \in \mathbf{G}$. By virtue of (F.a) and the remark preceding the statement of the theorem $\alpha \circ \tau^\ell \in \widehat{\mathbf{G}}$ for all $\ell \geq 0$. Since τ has finite order $\alpha \circ \tau^{-1} \in \widehat{\mathbf{G}}$. This means $f(\mathbf{g}) \in \mathcal{G}$ as well. Now $\mathbf{g}^N = 1$ by (F.c). Thus $f(\mathbf{g})^N = 1$.

Since $\boldsymbol{\lambda}$ has order N there is a Hopf algebra map $g : k[\mathbf{U}] \longrightarrow k[\mathcal{G}]$ determined by $g(\boldsymbol{\lambda}) = f(\mathbf{g})$. To show that $(g, f) \in \mathcal{F}_{k[\mathcal{G}], k[\mathbf{U}]}^\bullet$ we need only show that the conditions (a) – (e) of Corollary 8 are satisfied for f and g . Since \mathcal{G} is abelian (d) is satisfied. Using the fact that $\boldsymbol{\theta}$ is an algebra map,

(F.a), and (F.b), we compute

$$\theta(g(\lambda))e_{\tau(\sigma(s))} = \theta(g(\lambda))e_{\tau(s)} = \alpha(s)e_{\sigma(\tau(s))} = \alpha(\sigma(s))e_{\tau(\sigma(s))}$$

for all $s \in \mathbf{G}$. Therefore $\theta(g(\lambda))e_{\tau(s)} = \alpha(s)e_{\tau(s)} = g(\lambda)e_{\tau(s)}$ for all $s \in \mathbf{G}$ which implies $\theta(g(\lambda)) = g(\lambda)$. Since λ generates $k[\mathbf{U}]$ as an algebra $\theta \circ g = g$. Therefore condition (e) is met.

We observe $\tau(\mathbf{0}) = \mathbf{0}$ by (F.d); note that $\ell_\alpha(s, s) = 0$ for all $s \in \mathbf{G}$. The first equation is equivalent to $\epsilon \circ f = \epsilon$. Thus condition (a) is fulfilled. Lemma 4 and (F.a) account for the fact that condition (c) holds. As for (b), the reader is left to showing it is fulfilled by retracing the calculations following (8.13). We have shown $(g, f) \in \mathcal{F}_{k[\mathcal{G}], k[\mathbf{U}]}^\bullet$. The association $(\tau, \alpha) \mapsto (f, g)$ defines a function $\mathbf{g} : \mathcal{F}_{\mathbf{G}, \sigma, \lambda} \longrightarrow \mathcal{F}_{k[\mathcal{G}], k[\mathbf{U}]}^\bullet$. It is an easy exercise to show that \mathbf{f} and \mathbf{g} are inverse functions. This completes our proof of part (a).

Let F be as in part (b). Since $F_L = f$ and $F_R = g$ are algebra maps and $k[\mathcal{G}]$ is commutative

$$\begin{aligned} F(e_s \times \lambda^\ell) &= F_L(e_s)F_R(\lambda^\ell) \times \lambda^\ell \\ &= g(\lambda)^\ell f(e_s) \times \lambda^\ell \\ &= \alpha(s)^\ell e_{\tau(s)} \times \lambda^\ell. \end{aligned}$$

Since the $e_s \times \lambda^\ell$'s described in part (b) form a basis for A' , the proof of part (b) is complete. \square

9. THE GROUP $\Gamma(\mathbf{G}, \lambda, \sigma)$

In this section we recast the study of the group $\text{Aut}_{\text{Hopf}}(A', \pi')$, where $A' = k[\mathcal{G}] \times k[\mathbf{U}]$ is the biproduct of Theorem 8, in terms of permutations and characters. We continue with the notation of the previous section.

Let \mathcal{G} be any finite abelian group and $\sigma \in \text{Aut}_{\text{Group}}(\mathbf{G})$. Assume that k contains a primitive N^{th} root of unity λ , where $N = |\sigma|$ is the order of σ . Then we define

$$\Gamma(\mathbf{G}, \lambda, \sigma) = \{\tau \mid (\tau, \alpha) \in \mathcal{F}_{\mathbf{G}, \sigma, \lambda} \text{ for some } \alpha \in \widehat{\mathbf{G}}\}$$

We leave it to the reader to show that $\Gamma(\mathbf{G}, \lambda, \sigma)$ is a subgroup of $\text{Sym}(\mathbf{G})$. Observe that group $\text{Aut}_\sigma(\mathbf{G})$ of automorphisms of \mathbf{G} which commute with σ is a subgroup of $\Gamma(\mathbf{G}, \lambda, \sigma)$. The function

$$(9.1) \quad \nu_{\mathbf{G}, \sigma} : \mathcal{F}_{\mathbf{G}, \sigma, \lambda} \longrightarrow \Gamma(\mathbf{G}, \lambda, \sigma) \quad (\tau, \alpha) \mapsto \tau$$

is a bijection. By definition $\nu_{\mathbf{G}, \sigma}$ is onto. To see that it is one-one suppose $(\tau, \alpha), (\tau, \alpha') \in \mathcal{F}_{\mathbf{G}, \sigma, \lambda}$. Since τ is one-one $\ell_\alpha = \ell_{\alpha'}$ by (F.d). Fix $\mathbf{m} \in \mathbf{G}$. Then by (F.d) again

$$(\alpha(s)/\alpha(\mathbf{m}))^{N/|\mathbf{m}|} = (\alpha'(s)/\alpha'(\mathbf{m}))^{N/|\mathbf{m}|},$$

or equivalently

$$(\alpha(s)/\alpha'(s))^{N/|\mathbf{m}|} = (\alpha(\mathbf{m})/\alpha'(\mathbf{m}))^{N/|\mathbf{m}|},$$

for all $\mathbf{s} \in \mathbf{G}$. Therefore $\beta \in \widehat{\mathbf{G}}$ defined by $\beta(\mathbf{s}) = (\alpha(\mathbf{s})/\alpha'(\mathbf{s}))^{N/|\mathbf{m}|}$ for all $\mathbf{s} \in \mathbf{G}$ is constant. Hence $\beta = 1$ which means $(\alpha(\mathbf{s})/\alpha'(\mathbf{s}))^{N/|\mathbf{m}|} = 1$. Since N is the least common multiple of the lengths of the (σ) -orbits of \mathbf{G} it follows that $\alpha(\mathbf{s})/\alpha'(\mathbf{s}) = 1$. We have shown $\alpha = \alpha'$ and therefore $\nu_{\mathbf{G},\sigma}$ is one-one.

Theorem 9. *Let $A = k[\mathcal{G}] \times k[G]$ be the biproduct of Theorem 7. Then k contains a primitive N^{th} root of unity λ , where $N = |\theta|$. Assume further that k contains a primitive $|\mathcal{G}|^{\text{th}}$ root of unity. Let $A' = k[\mathcal{G}] \times k[\mathbf{U}]$ and let \mathbf{G} be the additive version of \mathcal{G} . Then:*

(a) *There is an isomorphism of groups*

$$\Phi_{A',\mathbf{G}} : \text{Aut}_{\text{Hopf}}(A', \pi') \longrightarrow \Gamma(\mathbf{G}, \lambda, \sigma)$$

for some $\sigma \in \text{Aut}_{\text{Group}}(\mathbf{G})$.

(b) *Let $F \in \text{Aut}_{\text{Hopf}}(A', \pi')$. Then F_L is a coalgebra map if and only if $\Phi_{A',\mathbf{G}}(F) \in \text{Aut}_{\text{Group}}(\mathbf{G})$.*

PROOF: $\Phi_{A',\mathbf{G}}$ is the composition of bijections

$$\text{Aut}_{\text{Hopf}}(A', \pi') \longrightarrow \mathcal{F}_{k[\mathcal{G}],k[\mathbf{U}]}^{\bullet} \longrightarrow \mathcal{F}_{\mathbf{G},\sigma,\lambda} \longrightarrow \Gamma(\mathbf{G}, \lambda, \sigma),$$

where the first is the inverse of the one of part (a) of Theorem 1, the second is the one of part (a) of Theorem 8, and the third is that of (9.1). Let $F \in \text{Aut}_{\text{Hopf}}(A', \pi')$. The calculation $F \mapsto (F_L, F_R) \mapsto (F_\tau, \alpha) \mapsto \tau$, where $F_L = F_\tau$ shows that $\Phi_{A',\mathbf{G}}(F) = \tau$. Note that F_L is a coalgebra map if and only if $\tau \in \text{Aut}_{\text{Group}}(\mathbf{G})$ by Lemma 4. \square

We continue with our general discussion of $\Gamma(\mathbf{G}, \lambda, \sigma)$. Let $\tau \in \Gamma(\mathbf{G}, \lambda, \sigma)$ and let $\alpha \in \widehat{\mathbf{G}}$ satisfy $(\tau, \alpha) \in \mathcal{F}_{\mathbf{G},\sigma,\lambda}$. Since $\alpha^N = 1$ it follows that $\text{Im}(\alpha) = (\omega)$, where $\omega \in k^\times$ is a primitive r^{th} root of unity where $r|N$. For $i \in \mathbb{Z}_r$ let $\mathbf{G}_i = \alpha^{-1}(\omega^i)$. Then $\mathbf{G}_0 = \text{Ker}(\alpha)$ and the \mathbf{G}_i 's are the cosets of \mathbf{G}_0 . Note that $\mathbf{G}_i + \mathbf{G}_j = \mathbf{G}_{i+j}$ for all $i, j \in \mathbb{Z}_r$, where addition of subscripts takes place in \mathbb{Z}_r . Also

$$(9.2) \quad \sigma(\mathbf{G}_i) = \mathbf{G}_i$$

for all $i \in \mathbb{Z}_r$ since $\alpha \circ \sigma = \alpha$. A consequence of (9.2) is that each \mathbf{G}_i is the union of (σ) -orbits of \mathbf{G} . For all $i \in \mathbb{Z}_r$ observe that (F.d) implies

$$(9.3) \quad \tau(\mathbf{s} - \mathbf{s}') = \tau(\mathbf{s}) - \tau(\mathbf{s}') \quad \text{for all } \mathbf{s}, \mathbf{s}' \in \mathbf{G}_i$$

as $\ell_\alpha(\mathbf{s}, \mathbf{s}') = 0$ for such \mathbf{s}, \mathbf{s}' . As a result

$$(9.4) \quad \tau(\mathbf{s} - \mathbf{m}) = \tau(\mathbf{s}) - \tau(\mathbf{m}) \quad \text{and} \quad \tau(\mathbf{s} + \mathbf{m}) = \tau(\mathbf{s}) + \tau(\mathbf{m})$$

for all $\mathbf{s} \in \mathbf{G}$ and $\mathbf{m} \in \mathbf{G}_0$.

PROOF: Let $\mathbf{s} \in \mathbf{G}$. Then $\mathbf{s} \in \mathbf{G}_i$ for some $i \in \mathbb{Z}_r$. Let $\mathbf{m} \in \mathbf{G}_0$. Then $\mathbf{s}, \mathbf{s} - \mathbf{m} \in \mathbf{G}_i$ and thus $\tau(\mathbf{m}) = \tau(\mathbf{s} - (\mathbf{s} - \mathbf{m})) = \tau(\mathbf{s}) - \tau(\mathbf{s} - \mathbf{m})$ by (9.3) from which the first equation of (9.4) follows. As for the second we use the

first to calculate $\tau(\mathbf{s}) = \tau((\mathbf{s} + \mathbf{m}) - \mathbf{m}) = \tau(\mathbf{s} + \mathbf{m}) - \tau(\mathbf{m})$ from which the second equation of (9.4) follows. \square

Let $\mathbf{s}, \mathbf{s}' \in \mathbf{G}$ and $\mathbf{m}, \mathbf{m}' \in \mathbf{G}_0$. It follows from (9.4) and (F.d) that

$$\begin{aligned} \tau((\mathbf{s} + \mathbf{m}) - (\mathbf{s}' + \mathbf{m}')) &= \tau((\mathbf{s} - \mathbf{s}') + (\mathbf{m} - \mathbf{m}')) \\ &= \tau(\mathbf{s}) - \tau(\sigma^{\ell_\alpha(\mathbf{s}, \mathbf{s}')}(\mathbf{s}')) + \tau(\mathbf{m}) - \tau(\mathbf{m}') \\ &= \tau(\mathbf{s} + \mathbf{m}) - \tau(\sigma^{\ell_\alpha(\mathbf{s}, \mathbf{s}')}(\mathbf{s}') + \mathbf{m}') \end{aligned}$$

on the one hand and

$$\tau((\mathbf{s} + \mathbf{m}) - (\mathbf{s}' + \mathbf{m}')) = \tau(\mathbf{s} + \mathbf{m}) - \tau(\sigma^{\ell_\alpha(\mathbf{s} + \mathbf{m}, \mathbf{s}' + \mathbf{m}')}(\mathbf{s}' + \mathbf{m}'))$$

on the other. Since τ is one-one

$$(9.5) \quad \sigma^{\ell_\alpha(\mathbf{s} + \mathbf{m}, \mathbf{s}' + \mathbf{m}')}(\mathbf{s}' + \mathbf{m}') = \sigma^{\ell_\alpha(\mathbf{s}, \mathbf{s}')}(\mathbf{s}') + \mathbf{m}'.$$

Lemma 6. *Let $\tau \in \mathcal{F}_{\mathbf{G}, \sigma, \lambda}$, let $\mathbf{s}, \mathbf{s}' \in \mathbf{G}$, let $\mathbf{m}, \mathbf{m}' \in \mathbf{G}_0$, and let r be the order of α . Then:*

- (a) $\ell_\alpha(\mathbf{s}, \mathbf{m}) = 0$.
- (b) $\ell_\alpha(\mathbf{s}, \mathbf{s}') = 0$ when $\mathbf{s}, \mathbf{s}' \in \mathbf{G}_i$ for some $i \in \mathbb{Z}_r$.
- (c) $\sigma^{\ell_\alpha(\mathbf{s} + \mathbf{m}, \mathbf{s}')}(\mathbf{s}') = \sigma^{\ell_\alpha(\mathbf{s}, \mathbf{s}' - \mathbf{m}')}(\mathbf{s}' - \mathbf{m}') + \mathbf{m}'$.
- (d) $\ell_\alpha(\mathbf{s} + \mathbf{m}, \mathbf{s}') = \ell_\alpha(\mathbf{s}, \mathbf{s}')$.
- (e) $\alpha(\mathbf{s})^{N/|\mathbf{m}|} = 1$; thus $|\mathbf{m}|$ divides N/r .
- (f) *If the lengths of (σ) -orbits of \mathbf{G} are the lengths of the (σ) -orbits of \mathbf{G}_0 then $\alpha = 1$, that is $\tau \in \text{Aut}_{\text{Group}}(\mathbf{G})$.*

PROOF: $\tau(\mathbf{s} - \mathbf{s}') = \tau(\mathbf{s}) - \tau(\mathbf{s}')$ if and only if $\ell_\alpha(\mathbf{s}, \mathbf{s}') = 0$ by (F.d) since τ is one-one. Thus part (a) follows by (9.4). We have noted part (b) holds. Part (c) is a reformulation of (9.5). As for part (d) we note that part (c) is $\sigma^{\ell_\alpha(\mathbf{s} + \mathbf{m}, \mathbf{s}')}(\mathbf{s}') = \sigma^{\ell_\alpha(\mathbf{s}, \mathbf{s}')}(\mathbf{s}')$ when we take $\mathbf{m}' = \mathbf{0}$. Thus part (d) follows by (F.d).

By part (a) and (F.d) we have $\alpha(\mathbf{s})^{N/|\mathbf{m}|} = 1$. Therefore r divides $N/|\mathbf{m}|$ which means $|\mathbf{m}|$ divides N/r . We have established part (e).

Assume the hypothesis of part (f). Since N is the least common multiple of the lengths of the (σ) -orbits of \mathbf{G} , by part (e) it follows that N divides N/r . Therefore $r = 1$ which means $\alpha = 1$. Consequently $\mathbf{G} = \mathbf{G}_0$ and therefore $\ell_\alpha(\mathbf{s}, \mathbf{s}') = 0$ by part (a). We have noted this equation is equivalent to $\tau(\mathbf{s} - \mathbf{s}') = \tau(\mathbf{s}) - \tau(\mathbf{s}')$. The latter implies τ is a group homomorphism. \square

Part (f) of the preceding lemma suggests examination of the relationship between the lengths of the (σ) -orbits of \mathbf{G} and those of the (σ) -orbits of \mathbf{G}_0 . Let $\mathbf{s} \in \mathbf{G}$. Then $\mathbf{s} \in \mathbf{G}_i$ for some $i \in \mathbb{Z}_r$. Since $\sigma(\mathbf{s}) \in \mathbf{G}_i$ by (9.2), we have $\sigma(\mathbf{s}) = \mathbf{s} + \mathbf{m}$ for some $\mathbf{m} \in \mathbf{G}_0$. Thus

$$\sigma^\ell(\mathbf{s}) = \mathbf{s} + \mathbf{m} + \cdots + \sigma^{\ell-1}(\mathbf{m})$$

for all $\ell \geq 1$. In particular $\mathbf{s} = \sigma^{|\mathbf{s}|}(\mathbf{s}) = \mathbf{s} + \mathbf{m} + \cdots + \sigma^{|\mathbf{s}|-1}(\mathbf{m})$ which means $\mathbf{m} + \cdots + \sigma^{|\mathbf{s}|-1}(\mathbf{m}) = \mathbf{0}$. Therefore $\sigma^{|\mathbf{s}|}(\mathbf{m}) = \mathbf{m}$ from which we conclude $|\mathbf{m}|$ divides $|\mathbf{s}|$. We have shown $|\mathbf{s}| = s|\mathbf{m}|$ for some positive integer.

Let $\mathbf{f} = \mathbf{m} + \cdots + \sigma^{|\mathbf{m}|-1}(\mathbf{m})$. Then $\mathbf{f} \in \mathbf{G}_0$, $\sigma(\mathbf{f}) = \mathbf{f}$, and $\sigma^{|\mathbf{m}|}(\mathbf{s}) = \mathbf{s} + \mathbf{f}$. The latter implies $\sigma^{\ell|\mathbf{m}|}(\mathbf{s}) = \mathbf{s} + \ell\mathbf{f}$ for all non-negative integers ℓ . Therefore $s\mathbf{f} = 0$ and if ℓ is a positive integer such that $\ell\mathbf{f} = 0$ then s divides ℓ . To summarize:

Lemma 7. *Let $\mathbf{s} \in \mathbf{G}$. Then $\sigma(\mathbf{s}) = \mathbf{s} + \mathbf{m}$ for some $\mathbf{m} \in \mathbf{G}_0 = \text{Ker}(\alpha)$. Set $\mathbf{f} = \mathbf{m} + \cdots + \sigma^{|\mathbf{m}|-1}(\mathbf{m})$. Then:*

- (a) $\mathbf{f} \in \mathbf{G}_0$ and $\sigma(\mathbf{f}) = \mathbf{f}$;
- (b) $|\mathbf{s}| = s|\mathbf{m}|$, where s is the order of \mathbf{f} .

□

Theorem 10. *Let \mathbf{G} be a finite abelian group, suppose $\sigma \in \text{Aut}_{\text{Group}}(\mathbf{G})$ and has order N , and suppose k has a primitive N^{th} root of unity λ . Then $\text{Aut}_{\sigma}(\mathbf{G}) = \Gamma(\mathbf{G}, \lambda, \sigma)$ if any of the following hold:*

- (a) σ has a unique fixed point.
- (b) The orders of σ and $|\mathbf{G}|$ are relatively prime.
- (c) N is prime N^2 does not divide $|\mathbf{G}|$.

PROOF: We have noted that $\text{Aut}_{\sigma}(\mathbf{G}) \leq \Gamma(\mathbf{G}, \lambda, \sigma)$. Let $\tau \in \Gamma(\mathbf{G}, \lambda, \sigma)$. Then $(\tau, \alpha) \in \mathcal{F}_{\mathbf{G}, \sigma, \lambda}$ for some $\alpha \in \hat{\mathbf{G}}$.

First of all assume part (a) or (b) holds. By Lemma 7 the hypothesis of part (f) of Lemma 6 holds. Therefore $\tau \in \text{Aut}_{\sigma}(\mathbf{G})$.

Now assume that part (c) holds and set $N = p$. Suppose $\tau \notin \text{Aut}_{\sigma}(\mathbf{G})$. Then $\alpha \neq 1$ by (F.d) which means α has order p by (F.c). Since a (σ) -orbit of \mathbf{G} has length 1 or p , \mathbf{G}_0 consists of fixed points of σ by part (f) of Lemma 6 again.

Let $\mathbf{s} \in \mathbf{G}$. Then $\sigma(\mathbf{s}) = \mathbf{s} + \mathbf{m}$ for some $\mathbf{m} \in \mathbf{G}_0$ by Lemma 7. Since $\sigma(\mathbf{m}) = \mathbf{m}$ it follows that $\mathbf{s} = \sigma^p(\mathbf{s}) = \mathbf{s} + p\mathbf{m}$ and therefore $p\mathbf{m} = \mathbf{0}$. Since $|\mathbf{G}| = p|\mathbf{G}_0|$ it follows p does not divide $|\mathbf{G}_0|$ since p^2 does not divide $|\mathbf{G}|$. Therefore $\mathbf{m} = \mathbf{0}$ which means $\sigma(\mathbf{s}) = \mathbf{s}$. We have shown $\sigma = \text{Id}_{\mathbf{G}}$, a contradiction. Therefore $\tau \in \text{Aut}_{\sigma}(\mathbf{G})$ after all. □

Closer examination of the proof of part (a) of the preceding theorem reveals:

Corollary 10. *Let $(\tau, \alpha) \in \mathcal{F}_{\mathbf{G}, \sigma, \lambda}$. If $\mathbf{0}$ is the only fixed point of σ in \mathbf{G}_0 then $\tau \in \text{Aut}_{\text{Group}}(\mathbf{G})$.* □

We construct examples where $\text{Aut}_{\sigma}(\mathbf{G}) < \Gamma(\mathbf{G}, \lambda, \sigma)$. To do this we examine what it means for $(\tau, \alpha) \in \mathcal{F}_{\mathbf{G}, \sigma}$, where σ has prime order $N = p$ and $\tau \notin \text{Aut}_{\sigma}(\mathbf{G})$. At one point we find it convenient to place a restriction on τ . We continue with the preceding notation and results of this section without particular reference for the most part.

Let \mathbf{G} be a finite abelian group, $\sigma \in \text{Aut}_{\text{Group}}(\mathbf{G})$ and has prime order p , and $(\tau, \alpha) \in \mathcal{F}_{\mathbf{G}, \sigma}$.

Suppose $\tau \notin \text{Aut}_{\text{Group}}(\mathbf{G})$. Then $\alpha \neq 1$. Since $\alpha^p = 1$ it follows that α has order p . We take $\omega = \lambda$. Thus $\mathbf{G}_i = \alpha^{-1}(\lambda^i)$ for all $0 \leq i \leq p-1$.

The (σ) -orbits of \mathbf{G} have lengths 1 or p . Now each \mathbf{G}_i is the union of (σ) -orbits since $\sigma(\mathbf{G}_i) = \mathbf{G}_i$. Since $\tau \notin \text{Aut}_{\text{Group}}(\mathbf{G})$, by part (f) of Lemma 6 it follows that \mathbf{G}_0 consists of fixed points of σ . The set \mathbf{F} of fixed points of σ is a subgroup of \mathbf{G} . Since $\mathbf{G}_0 \subseteq \mathbf{F}$ and $[\mathbf{G} : \mathbf{G}_0]$ is prime, either $\mathbf{F} = \mathbf{G}_0$ or $\mathbf{F} = \mathbf{G}$. Thus $\mathbf{F} = \mathbf{G}_0$ since $\sigma \neq \text{Id}_{\mathbf{G}}$. Since τ and σ commute and τ is bijective, $\tau(\mathbf{F}) = \mathbf{F}$. We have shown $\tau(\mathbf{G}_0) = \mathbf{G}_0$. The equation $\mathbf{F} = \mathbf{G}_0$ implies that \mathbf{G}_i is the union of (σ) -orbits of length p , where $1 \leq i \leq p-1$.

Each $\tau(\mathbf{G}_i)$ is a coset of $\tau(\mathbf{G}_0) = \mathbf{G}_0$ by (9.4). Therefore there is a $\eta \in \text{Sym}(\mathbb{Z}_p)$ such that

$$(9.6) \quad \eta(0) = 0 \text{ and } \tau(\mathbf{G}_i) = \mathbf{G}_{\eta(i)}$$

for all $0 \leq i \leq p-1$.

Now \mathbf{G}/\mathbf{G}_0 is cyclic of order p . Fix $\mathbf{s} \in \mathbf{G}_1$. Then $\mathbf{G}_i = i\mathbf{s} + \mathbf{G}_0$ for all $0 \leq i \leq p-1$. Since $\sigma(\mathbf{G}_1) = \mathbf{G}_1$,

$$(9.7) \quad \sigma(\mathbf{s}) = \mathbf{s} + \mathbf{m}$$

for some $\mathbf{m} \in \mathbf{G}_0$. Since $\sigma \neq \text{Id}_{\mathbf{G}}$ necessarily $\mathbf{m} \neq \mathbf{0}$. Since $\mathbf{s} = \sigma^p(\mathbf{s}) = \mathbf{s} + p\mathbf{m}$ we have shown

$$(9.8) \quad \mathbf{m} \neq \mathbf{0} \text{ and } p\mathbf{m} = \mathbf{0}.$$

Let $\tau_0 = \tau|_{\mathbf{G}_0}$. Since $\tau(\mathbf{G}_0) = \mathbf{G}_0$, by (9.4) again

$$(9.9) \quad \tau_0 \in \text{Aut}_{\text{Group}}(\mathbf{G}_0).$$

Let $0 \leq i \leq p-1$. Since $\tau(\mathbf{G}_i) = \mathbf{G}_{\eta(i)}$, which follows by (9.6), we have

$$(9.10) \quad \tau(i\mathbf{s}) = \eta(i)\mathbf{s} + \mathbf{n}_i$$

for some $\mathbf{n}_i \in \mathbf{G}_0$. Using (9.4) again, we deduce $\tau(\mathbf{0}) = \mathbf{0}$ and thus

$$(9.11) \quad \mathbf{n}_0 = \mathbf{0},$$

and also since σ is a homomorphism

$$(9.12) \quad \tau(i\mathbf{s} + \mathbf{x}) = \eta(i)\mathbf{s} + \mathbf{n}_i + \tau_0(\mathbf{x}) \text{ and } \sigma(i\mathbf{s} + \mathbf{x}) = i\mathbf{s} + i\mathbf{m} + \mathbf{x}$$

for all $0 \leq i \leq p-1$ and $\mathbf{x} \in \mathbf{G}_0$. The last two equations describe τ and σ explicitly.

Since τ and σ commute, (9.12) implies $\tau_0(i\mathbf{m}) = \eta(i)\mathbf{m}$ for all $0 \leq i \leq p-1$. Thus by virtue of (9.9) we have $\eta(i)\mathbf{m} = \tau_0(i\mathbf{m}) = i\tau_0(\mathbf{m}) = i\eta(1)\mathbf{m}$. Now $\mathbf{m} \neq \mathbf{0}$ and has order p by (9.7). We have shown

$$(9.13) \quad \eta(i) \equiv i\eta(1) \pmod{p} \text{ and } \tau_0(i\mathbf{m}) = i\eta(1)\mathbf{m}$$

for $0 \leq i \leq p-1$.

We now turn our attention to (F.d). Let $\mathbf{x}, \mathbf{x}' \in \mathbf{G}$. Then

$$(9.14) \quad \tau(\mathbf{x} - \mathbf{x}') = \tau(\mathbf{x}) - \tau(\sigma^{\ell_\alpha(\mathbf{x}, \mathbf{x}')}(\mathbf{x}')).$$

We first determine $\ell_\alpha(\mathbf{x}, \mathbf{x}')$. Now $\mathbf{x} \in \mathbf{G}_i$ and $\mathbf{x}' \in \mathbf{G}_{i'}$, where $0 \leq i, i' \leq p-1$. Since $\ell_\alpha(\mathbf{x}, \mathbf{x}') = 0$ when $i' = 0$ we will assume $1 \leq i'$. Hence $|\mathbf{x}'| = p$. Therefore the equation

$$(\alpha(\mathbf{x})/\alpha(\mathbf{x}'))^{p/|\mathbf{x}'|} = \lambda_{|\mathbf{x}'|}^{\ell_\alpha(\mathbf{x}, \mathbf{x}')}(\mathbf{x}')$$

is $\lambda^{i-i'} = \lambda^{\ell_\alpha(\mathbf{x}, \mathbf{x}')}.$ We have therefore

$$(9.15) \quad \ell_\alpha(\mathbf{x}, \mathbf{x}') \equiv i - i' \pmod{p} \text{ and } 0 \leq \ell_\alpha(\mathbf{x}, \mathbf{x}') \leq p-1$$

for all $\mathbf{x} \in \mathbf{G}_i, \mathbf{x}' \in \mathbf{G}_{i'}$ and $0 \leq i, i' \leq p-1, 1 \leq i'.$ Since $\sigma^j(i'\mathbf{s}) = i'\mathbf{s} + ji'\mathbf{m}$ for all $j \in \mathbb{Z}$, when $\mathbf{x} = i\mathbf{s}$ and $\mathbf{x}' = i'\mathbf{s}'$, (9.14) and (9.15) imply

$$\begin{aligned} \tau((i - i')\mathbf{s}) &= \tau(i\mathbf{s} - i'\mathbf{s}) \\ &= \tau(i\mathbf{s}) - \tau(\sigma^{\ell_\alpha(i\mathbf{s}, i'\mathbf{s}')} (i'\mathbf{s})) \\ &= \tau(i\mathbf{s}) - \tau(\sigma^{i-i'} (i'\mathbf{s})) \\ &= \tau(i\mathbf{s}) - \tau(i'\mathbf{s} + (i - i')i'\mathbf{m}). \end{aligned}$$

Therefore

$$(9.16) \quad \tau((i - i')\mathbf{s}) = (\eta(i) - \eta(i'))\mathbf{s} + (\mathbf{n}_i - \mathbf{n}_{i'}) - (i - i')i'\eta(1)\mathbf{m}$$

for all $0 \leq i, i' \leq p-1$ and $1 \leq i'$ by (9.12) and (9.13).

We consider what it means for (9.16) to hold. It holds when $i = i'.$ There are two other cases.

Case 1: $1 \leq i' < i \leq p-1.$

In this situation (9.16) is

$$(9.17) \quad \eta(i - i')\mathbf{s} + \mathbf{n}_{i-i'} = (\eta(i) - \eta(i'))\mathbf{s} + (\mathbf{n}_i - \mathbf{n}_{i'}) - (i - i')i'\eta(1)\mathbf{m}.$$

This equation implies $\eta(i - i') - (\eta(i) - \eta(i')) \equiv 0 \pmod{p}$ which is already implied by (9.13). The restriction we wish to place on τ is

$$(ER) \quad \eta = \text{Id}_{\mathbb{Z}_p},$$

that is $\tau(\mathbf{G}_i) = \mathbf{G}_i$ for all $0 \leq i \leq p-1.$ Observe that (ER) holds when $p = 2.$ Also $\tau(\mathbf{G}_1) = \mathbf{G}_1$ implies (ER) by (9.13).

Under the assumption that (ER) holds (9.17) is

$$(9.18) \quad \mathbf{n}_{i-i'} = (\mathbf{n}_i - \mathbf{n}_{i'}) - (i - i')i'\eta(1)\mathbf{m}$$

for all $1 \leq i' < i \leq p-1.$ With $i' = 1$ the preceding equation can be written

$$(9.19) \quad \mathbf{n}_i = \mathbf{n}_{i-1} + \mathbf{n}_1 + (i-1)\eta(1)\mathbf{m}$$

for all $2 \leq i \leq p-1.$ We note here that (9.18) holds, and hence (9.19) also holds, when merely $p\mathbf{s} = \mathbf{0}.$ As a result of (9.19) we have

$$(9.20) \quad \mathbf{n}_i = i\mathbf{n}_1 + \binom{i}{2} \eta(1)\mathbf{m}$$

for $0 \leq i \leq p-1.$ This equation is $\mathbf{n}_i = \mathbf{n}_i$ for $i = 0, 1.$ For $2 \leq i$ the formula follows by induction on $i.$

Assume (9.20) holds. Then (9.18) holds by virtue of the identity

$$\binom{i - i'}{2} = \binom{i}{2} - \binom{i'}{2} - (i - i')i'$$

for all $0 \leq i' \leq i.$

Case 2: $0 \leq i < i' \leq p-1.$

In this case $i - i' = -p + r$, where $1 \leq r \leq p - 1$. Since $p\mathbf{s} \in \mathbf{G}_0$, the left hand side of (9.16) is

$$\begin{aligned} \tau((i - i')\mathbf{s}) &= \tau(-p\mathbf{s} + r\mathbf{s}) \\ &= \tau(-p\mathbf{s}) + \tau(r\mathbf{s}) \\ &= \tau(-p\mathbf{s}) + \tau((p + i - i')\mathbf{s}) \\ &= \tau(-p\mathbf{s}) + \eta(p + i - i')\mathbf{s} + \mathbf{n}_{p+i-i'}. \end{aligned}$$

Therefore (9.16) becomes, with the restriction (ER) holding,

$$\begin{aligned} (9.21) \quad \tau(-p\mathbf{s}) + p\mathbf{s} + p\mathbf{n}_1 + \binom{p+i-i'}{2} \mathbf{m} \\ = \left(\binom{i}{2} - \binom{i'}{2} - (i - i')i' \right) \mathbf{m}. \end{aligned}$$

Since

$$\binom{p+i-i'}{2} = \binom{p}{2} + \binom{i}{2} - \binom{i'}{2} - (i' - p)(i - i')$$

for all $0 \leq i < i' \leq p - 1$, and $p\mathbf{m} = \mathbf{0}$, in Case 2, under the assumption (ER) holds, (9.16) is

$$(9.22) \quad \tau_0(p\mathbf{s}) = p\mathbf{s} + p\mathbf{n}_1 + \binom{p}{2} \mathbf{m}.$$

When $p = 2$ this equation is $\tau(2\mathbf{s}) = 2\mathbf{s} + 2\mathbf{n}_1 + \mathbf{m}$ and when $p > 2$ this equation is $\tau(p\mathbf{s}) = p\mathbf{s} + p\mathbf{n}_1$.

Proposition 3. *Let p be a prime integer and suppose k contains a primitive p^{th} root of unity λ . Let \mathbf{G} be a finite abelian group with a subgroup \mathbf{G}_0 of index p . Let $\mathbf{s} \in \mathbf{G}$ satisfy $\mathbf{s} + \mathbf{G}$ generates \mathbf{G}/\mathbf{G}_0 .*

- (a) *Suppose $\mathbf{m} \in \mathbf{G}_0$ satisfies $\mathbf{m} \neq \mathbf{0}$ and $p\mathbf{m} = \mathbf{0}$. Then there exists $\sigma \in \text{Aut}_{\text{Group}}(\mathbf{G})$ determined by $\sigma(\mathbf{s}) = \mathbf{s} + \mathbf{m}$ and $\sigma(\mathbf{x}) = \mathbf{x}$ for all $\mathbf{x} \in \mathbf{G}_0$. In particular σ has order p .*
- (b) *Let \mathbf{m} be as in part (a). Suppose $\tau_0 \in \text{Aut}_{\text{Group}}(\mathbf{G}_0)$ satisfies $\tau_0(\mathbf{m}) = \mathbf{m}$ and there is an $\mathbf{n} \in \mathbf{G}_0$ such that $\tau_0(2\mathbf{s}) = 2\mathbf{s} + 2\mathbf{n} + \mathbf{m}$, if $p = 2$, and $\tau_0(p\mathbf{s}) = p\mathbf{s} + p\mathbf{n}$, if $p > 2$. Then $(\tau, \alpha) \in \mathcal{F}_{\mathbf{G}, \sigma}$, where τ is defined by*

$$\tau(i\mathbf{s} + \mathbf{x}) = i(\mathbf{s} + \mathbf{n}) + \binom{i}{2} \mathbf{m} + \tau_0(\mathbf{x})$$

for all $0 \leq i \leq p - 1$ and $\mathbf{x} \in \mathbf{G}_0$, and the character α is given by $\alpha(\mathbf{G}_i) = \{\lambda^i\}$ for all $0 \leq i \leq p - 1$. Furthermore $\tau \notin \text{Aut}_{\sigma}(\mathbf{G})$.

- (c) $\text{Aut}_{\sigma}(\mathbf{G}) < \Gamma(\mathbf{G}, \lambda, \sigma)$.

PROOF: The reader is left with the straightforward exercise of completing the proof of the proposition. \square

The conditions of Proposition 3 are met in the following example. Let $\mathbf{G} = \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p \oplus \mathbb{Z}_{p^2}$ where the number of \mathbb{Z}_p summands is at least one.

Let \mathbf{s} be a generator of \mathbb{Z}_{p^2} . Then $\mathbf{G}_0 = \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p \oplus (p\mathbf{s})$ is a subgroup of \mathbf{G} of index p and is a direct sum of copies of \mathbb{Z}_p . Observe that $p\mathbf{x} = \mathbf{0}$ for all $\mathbf{x} \in \mathbf{G}_0$.

Suppose $p > 2$. Take $\tau_0 = \text{Id}_{\mathbf{G}_0}$ and choose any $\mathbf{m}, \mathbf{n} \in \mathbf{G}_0$, where $\mathbf{m} \neq \mathbf{0}$. Then $\tau_0(p\mathbf{s}) = p\mathbf{s} = p\mathbf{s} + p\mathbf{n}$.

Now suppose $p = 2$. Choose a $\tau_0 \in \text{Aut}_{\text{Group}}(\mathbf{G}_0)$ such that the (τ_0) -orbit of $2\mathbf{s}$ has length 2. The function which permutes the last two summands of \mathbf{G}_0 is an example. Let $\mathbf{m} = \tau_0(2\mathbf{s}) - 2\mathbf{s}$. Then $\tau_0(2\mathbf{s}) = 2\mathbf{s} + \mathbf{m}$; hence $\mathbf{m} \in \mathbf{G}_0$, $\mathbf{m} \neq \mathbf{0}$, and $2\mathbf{m} = \mathbf{0}$. For any $\mathbf{n} \in \mathbf{G}_0$ observe that $\tau_0^2(2\mathbf{s}) = 2\mathbf{s} + 2\mathbf{n} + \mathbf{m}$.

When $p > 2$ the group $\mathbf{G} = \mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p$ which is the direct sum of n copies \mathbb{Z}_p , where $n \geq 2$, provides examples also. Here we take \mathbf{G}_0 to be the direct sum of the first $n - 1$ copies of \mathbb{Z}_p and \mathbf{s} to be a generator of the last copy. Choose any $\mathbf{m}, \mathbf{n} \in \mathbf{G}_0$, where $\mathbf{m} \neq \mathbf{0}$. Let $\tau_0 = \text{Id}_{\mathbf{G}_0}$. Since $p\mathbf{x} = \mathbf{0}$ for all $\mathbf{x} \in \mathbf{G}$ the equation $\tau_0(p\mathbf{s}) = p\mathbf{s} + p\mathbf{n}$ is trivially satisfied. We point out that $p\mathbf{m} = \mathbf{0}$ in this example.

10. THE BIPRODUCT OF SECTION 7 REVISITED

Here we apply results of Sections 6 and 9 to the biproduct of Section 7.

Theorem 11. *Let $A = k[\mathcal{G}] \times H$ be the biproduct of Theorem 7, where \mathcal{G} is a finite abelian group. Suppose k contains primitive $|\mathcal{G}|^{\text{th}}$ root of unity. Then the one-one group homomorphism*

$$\Phi_{\mathcal{YD}} : \mathcal{N}(B, H)^{\text{op}} \rtimes_{\varphi} \text{Aut}_{\mathcal{YD}\text{-Hopf}}(B) \longrightarrow \text{Aut}_{\text{Hopf}}(A, \pi)$$

of Theorem 5 is an isomorphism if any of the following hold:

- (a) θ fixes a unique one-dimensional ideal of $k[\mathcal{G}]$.
- (b) The orders of θ and $|\mathcal{G}|$ are relatively prime.
- (c) If θ has order p , where p is prime, and p^2 does not divide $|\mathcal{G}|$.

PROOF: We have noted that k contains a primitive $|\theta|^{\text{th}}$ root of unity λ . Let $A' = k[\mathcal{G}] \times k[\mathbf{U}]$. At this point we bring into play the group homomorphism $\Phi : \text{Aut}_{\text{Hopf}}(A, \pi) \longrightarrow \text{Aut}_{\text{Hopf}}(A', \pi')$ of Section 6 and the isomorphism $\Phi_{A', \mathbf{G}} : \text{Aut}_{\text{Hopf}}(A', \pi') \longrightarrow \Gamma(\mathbf{G}, \lambda, \sigma)$ of Theorem 9. The conditions (a)-(c) of Theorem 5 translate to the conditions (a)-(c) of Theorem 10 respectively. Thus $\Gamma(\mathbf{G}, \lambda, \sigma) = \text{Aut}_{\sigma}(\mathbf{G})$ by the same.

Let $F \in \text{Aut}_{\text{Hopf}}(A, \pi)$. Then $F_L = \Phi(F)_L$ is a coalgebra map by part (b) of Theorem 9. At this point the proof follows by Corollary 7. \square

Generally $\Phi_{\mathcal{YD}}$ is not an isomorphism.

Proposition 4. *Suppose k is an algebraically closed field of characteristic 0. Let p be a prime integer. Then there exists a biproduct $A = k[\mathcal{G}] \times k[\mathbb{Z}_p]$, where \mathcal{G} is a finite abelian group, such that:*

- (a) *The one-one group map $\Phi_{\mathcal{YD}}$ of Theorem 5 is not onto. In particular there is an $F \in \text{Aut}_{\text{Hopf}}(A, \pi)$ such that F_L is not a coalgebra map.*

- (b) *The one-one group map $\Phi_\nu : \mathcal{N}(B, H)^{op} \rtimes_{\varphi} \text{Im}(\nu) \longrightarrow \text{Sym}(A)$ of Theorem 6 satisfies $\text{Im}(\Phi_\nu) \not\subseteq \text{Aut}_{\text{Hopf}}(A, \pi)$.*

PROOF: In light of Theorems 5, 6, and 9 we need only find finite abelian groups \mathbf{G} such that $\text{Aut}_\sigma(\mathbf{G}) < \Gamma(\mathbf{G}, \lambda, \sigma)$, where σ has order p and $\lambda \in k^\times$ is a primitive p^{th} root of unity. Such examples are constructed after the proof of Proposition 3. \square

11. ANOTHER GROUP ASSOCIATED WITH $\Gamma(\mathbf{G}, \lambda, \sigma)$

Let G be an additive group and $\sigma \in \text{Aut}_{\text{Group}}(G)$. Let $\text{Aut}_\sigma(G)$ be the set of all $\tau \in \text{Aut}_{\text{Group}}(G)$ which commute with σ . Let $\text{Sym}_\sigma^-(G)$ be the set $\tau \in \text{Sym}(G)$ which satisfy $\tau \circ \sigma = \sigma \circ \tau$ and

$$(11.1) \quad \tau(a - \mathcal{O}) = \tau(a) - \tau(\mathcal{O})$$

for all $a \in G$ and (σ) -orbits \mathcal{O} of G . Observe that $\tau \in \text{Sym}_\sigma^-(G)$ permutes the (σ) -orbits of G since $\tau \circ \sigma = \sigma \circ \tau$. These four sets of permutations are groups under composition and their relationships are described by

$$\text{Aut}_\sigma(G) \leq \text{Aut}_{\text{Group}}(G) \leq \text{Sym}(G) \text{ and } \text{Aut}_\sigma(G) \leq \text{Sym}_\sigma^-(G) \leq \text{Sym}(G).$$

The group $\Gamma(\mathbf{G}, \lambda, \sigma)$ of Section 9 satisfies

$$\Gamma(\mathbf{G}, \lambda, \sigma) \leq \text{Sym}_\sigma^-(\mathbf{G}).$$

Since $\text{Sym}_\sigma^-(G)$ is such a natural generalization of $\Gamma(\mathbf{G}, \lambda, \sigma)$ perhaps there will be some interest in it.

In this section we derive some of the elementary properties of the group $\text{Sym}_\sigma^-(G)$ and describe examples such that $\Gamma(\mathbf{G}, \lambda, \sigma) < \text{Sym}_\sigma^-(\mathbf{G})$. Let $a \in G$. We let $|a|$ denote the cardinality of the (σ) -orbit of G which a generates.

The set F of fixed points of σ is a subgroup of G . Let $\tau \in \text{Sym}_\sigma^-(G)$. Then $\tau(F) = F$ since τ and σ commute and τ is bijective. Let $m \in F$ and $\tau \in \text{Sym}_\sigma^-(G)$. Observe that $\tau(a - m) = \tau(a) - \tau(m)$ for all $a \in G$ by (12.1) since $|m| = 1$. In particular $\tau(0) = \tau(0 - 0) = \tau(0) - \tau(0) = 0$ and thus $\tau(-m) = \tau(0 - m) = \tau(0) - \tau(m) = -\tau(m)$. As a consequence

$$(11.2) \quad \tau(a + m) = \tau(a) + \tau(m)$$

for all $a \in G$ and $m \in F$. Since $\tau(F) = F$ the last equation implies that τ permutes the left cosets of F in G and

$$(11.3) \quad \tau_0 \in \text{Aut}_{\sigma_0}(F),$$

For the remainder of this section \mathbf{G} , \mathbf{G}_0 , \mathbf{s} , and \mathbf{m} are as described in Proposition 3 and $G = \mathbf{G}$. Then $\mathbf{G}_i := i\mathbf{s} + \mathbf{G}_0$, $0 \leq i \leq p-1$, lists the cosets of \mathbf{G}_0 in \mathbf{G} . Recall that $\mathbf{m} \in \mathbf{G}_0$, $\mathbf{m} \neq \mathbf{0}$, and $p\mathbf{m} = \mathbf{0}$. Let $\sigma \in \text{Aut}_{\text{Group}}(\mathbf{G})$ be the automorphism determined by $\sigma(\mathbf{s}) = \mathbf{s} + \mathbf{m}$ and $\sigma(\mathbf{x}) = \mathbf{x}$ for $\mathbf{x} \in \mathbf{G}_0$. Then $F = \mathbf{G}_0$.

Since τ permutes the cosets of $F = \mathbf{G}_0$ in \mathbf{G} , and $\tau(\mathbf{G}_0) = \mathbf{G}_0$, there is an $\eta \in \text{Sym}(\mathbb{Z}_p)$ such that $\tau(\mathbf{G}_i) = \mathbf{G}_{\eta(i)}$ for all $0 \leq i \leq p-1$ and $\eta(0) = 0$. For $0 \leq i \leq p-1$ we have

$$(11.4) \quad \tau(i\mathbf{s}) = \eta(i)\mathbf{s} + \mathbf{n}_i$$

for all $0 \leq i \leq p-1$, where $\mathbf{n}_i \in \mathbf{G}_0$. We have shown $\tau(\mathbf{0}) = \mathbf{0}$. Therefore $\mathbf{n}_0 = \mathbf{0}$. Thus (11.2) and the fact that σ is a homomorphism imply that (9.12) holds, in particular

$$\tau(i\mathbf{s} + \mathbf{x}) = \eta(i)\mathbf{s} + \mathbf{n}_i + \tau_0(\mathbf{x})$$

for all $0 \leq i \leq p-1$ and $\mathbf{x} \in \mathbf{G}_0$. Since σ and τ commute (9.13) holds.

We now turn our attention to (12.1). Let $\mathbf{a}, \mathbf{a}' \in \mathbf{G}$. Then $\mathbf{a} \in \mathbf{G}_i$ and $\mathbf{a}' \in \mathbf{G}_{i'}$ for some $0 \leq i, i' \leq p-1$. Write $\mathbf{a} = i\mathbf{s} + \mathbf{x}$ and $\mathbf{a}' = i'\mathbf{s} + \mathbf{x}'$, where $\mathbf{x}, \mathbf{x}' \in \mathbf{G}_0$. Since $p\mathbf{m} = \mathbf{0}$, the (σ) -orbit of \mathbf{G} which \mathbf{a}' generates is

$$\mathcal{O} = \{i'\mathbf{s} + \ell i'\mathbf{m} + \mathbf{x}' \mid 0 \leq \ell \leq p-1\}.$$

Therefore (12.1) holds if and only if

$$\begin{aligned} & \{\tau((i-i')\mathbf{s}) - \ell i'\eta(1)\mathbf{m} \mid 0 \leq \ell \leq p-1\} \\ &= \{(\eta(i) - \eta(i'))\mathbf{s} + (\mathbf{n}_i - \mathbf{n}_{i'}) - \ell' i'\eta(1)\mathbf{m} \mid 0 \leq \ell' \leq p-1\} \end{aligned}$$

which holds if and only if

$$(11.5) \quad \tau((i-i')\mathbf{s}) = (\eta(i) - \eta(i'))\mathbf{s} + (\mathbf{n}_i - \mathbf{n}_{i'}) - \ell_{i,i'} i'\eta(1)\mathbf{m}$$

for some $0 \leq \ell_{i,i'} \leq p-1$. Observe that (11.5) holds when $i = i'$, with $\ell_{i,i} = 0$, and when $i' = 0$. We will therefore assume $1 \leq i'$.

From this point on we assume that (ER) holds; that is $\eta(i) = i$ for all $0 \leq i \leq p-1$. We note as a consequence of (9.13) that $\tau(\mathbf{m}) = \mathbf{m}$. There are two more cases to consider.

Case 1: $1 \leq i' < i \leq p-1$.

Since (ER) holds, in this situation (11.5) boils down to

$$\mathbf{n}_{i-i'} = \mathbf{n}_i - \mathbf{n}_{i'} - \ell_{i,i'} i'\mathbf{m}$$

in this case. When $i' = 1$ the preceding equation can be written

$$(11.6) \quad \mathbf{n}_i = \mathbf{n}_{i-1} + \mathbf{n}_1 + \ell_{i,1}\mathbf{m}$$

for all $1 \leq i \leq p-1$. Thus

$$\mathbf{n}_i = i\mathbf{n}_1 + \left(\sum_{u=2}^i \ell_{u,1} \right) \mathbf{m}$$

for all $0 \leq i \leq p-1$. For $1 \leq j < i \leq p-1$ we set

$$s(i, j) = \sum_{u=j+1}^i \ell_{u,1}$$

and set $s(i, j) = 0$ otherwise. We have shown:

$$(11.7) \quad \mathbf{n}_i = i\mathbf{n}_1 + s(i, 1)\mathbf{m}$$

for all $0 \leq i \leq p-1$. Therefore (11.5) can be rewritten

$$(11.8) \quad i' \ell_{i,i'} \mathbf{m} = (s(i, i-i') - s(i', 1)) \mathbf{m}$$

for all $1 \leq i' < i \leq p-1$. Since i' is a unit (mod p) and \mathbf{m} has order p there exists a unique solution $0 \leq \ell_{i,i'} \leq p-1$ to this equation in terms of the $s(i, j)$'s.

Case 2: $0 \leq i < i' \leq p-1$.

In this case $i-i' = -p+r$, where $1 \leq r \leq p-1$. Since $ps \in \mathbf{G}_0$ and (ER) holds, in this situation the left hand side of (11.5) is

$$\tau((i-i')\mathbf{s}) = \tau(-ps + rs) = \tau(-ps) + rs + \mathbf{n}_r$$

and therefore (11.5) boils down to

$$(11.9) \quad \tau_0(ps) - ps - p\mathbf{n}_1 = (s(p+i-i', 1) + s(i', i))\mathbf{m} + \ell_{i,i'} i' \mathbf{m}.$$

This equation has a solution $0 \leq \ell_{i,i'} \leq p-1$ if and only if

$$(11.10) \quad \tau_0(ps) - ps - p\mathbf{n}_1 \in \mathbb{Z}\mathbf{m}.$$

Again, such a solution must be unique.

Proposition 5. *Assume the hypothesis of Proposition 3. Suppose $\mathbf{m} \in \mathbf{G}_0$ satisfies $\mathbf{m} \neq \mathbf{0}$ and $p\mathbf{m} = \mathbf{0}$. Let $\sigma \in \text{Aut}_{\text{Group}}(\mathbf{G})$ be determined by $\sigma(\mathbf{s}) = \mathbf{s} + \mathbf{m}$ and $\sigma(\mathbf{x}) = \mathbf{x}$ for all $\mathbf{x} \in \mathbf{G}_0$.*

- (a) *Suppose $\tau_0 \in \text{Aut}_{\text{Group}}(\mathbf{G}_0)$ satisfies $\tau_0(\mathbf{m}) = \mathbf{m}$ and $\mathbf{n} \in \mathbf{G}_0$ is such that $\tau_0(ps) - ps - p\mathbf{n} \in \mathbb{Z}\mathbf{m}$. Let $0 \leq \ell_{2,1}, \dots, \ell_{p-1,1} \leq p-1$. Then there is a $\tau \in \text{Sym}_{\sigma}^{-}(\mathbf{G})$ given by*

$$\tau(is + \mathbf{x}) = i(\mathbf{s} + \mathbf{n}) + s(i, 1)\mathbf{m} + \tau_0(\mathbf{x})$$

for all $0 \leq i \leq p-1$ and $\mathbf{x} \in \mathbf{G}_0$, where $s(i, 1) = \sum_{u=2}^i \ell_{u,1}$ for all $0 \leq i \leq p-1$.

For the τ of part (a):

- (b) *If $\tau \in \text{Aut}_{\sigma}(\mathbf{G})$ then $\ell_{2,1} = \dots = \ell_{p-1,1} = 0$.*
(c) *If $\tau \in \Gamma(\mathbf{G}, \lambda, \sigma) \setminus \text{Aut}_{\sigma}(\mathbf{G})$ then $\ell_{i,1} = i-1$ for all $2 \leq i \leq p-1$.*

Furthermore

- (d) *$\text{Aut}_{\sigma}(\mathbf{G}) < \Gamma(\mathbf{G}, \lambda, \sigma) < \text{Sym}_{\sigma}^{-}(\mathbf{G})$ when $p \geq 3$.*

PROOF: Most of the details for the proof of part (a) can be gleaned from the discussion preceding the statement of the proposition. The reader is left with the short exercise of completing the proof. As for part (b), suppose that τ is a group homomorphism. Since $\tau(\mathbf{s}) = \mathbf{s} + \mathbf{n}$ it follows that $\tau(is) = is + i\mathbf{n}$ for all $0 \leq i \leq p-1$. Therefore $s(i, 1)\mathbf{m} = \mathbf{0}$ for all $0 \leq i \leq p-1$ which means $\ell_{i,1} = 0$ for all $2 \leq i \leq p-1$.

As for part (c), suppose $\tau \in \Gamma(\mathbf{G}, \lambda, \sigma) \setminus \text{Aut}_{\sigma}(\mathbf{G})$. As $\tau(\mathbf{G}_i) = \mathbf{G}_i$ it follows $\eta = \text{Id}_{\mathbb{Z}_p}$. Note that \mathbf{G}_0 is the set of fixed points of σ . By (9.20) we have $s(i, 1)\mathbf{m} = \binom{i}{2} \mathbf{m}$ for all $2 \leq i \leq p-1$. Therefore $\ell_{i,1} = i-1$ for all

$2 \leq i \leq p-1$. We have established part (c). Part (d) follows from parts (b) and (c). \square

The examples we constructed which realize Proposition 3 of course realize Proposition 5.

12. YET ANOTHER EXAMPLE OF $\text{Sym}_\sigma^-(G)$

Let G be an additive group and $\sigma \in \text{Aut}_{\text{Group}}(G)$. Let $\text{Sym}_\sigma^+(G)$ be the set of all $\tau \in \text{Sym}(G)$ which satisfy $\tau \circ \sigma = \sigma \circ \tau$ and

$$(12.1) \quad \tau(a + \mathcal{O}) = \tau(a) + \tau(\mathcal{O})$$

for all $a \in G$ and (σ) -orbits \mathcal{O} of G . Again, $\tau \in \text{Sym}_\sigma^+(G)$ permutes the (σ) -orbits of G since $\tau \circ \sigma = \sigma \circ \tau$. Thus $\text{Sym}_\sigma^+(G)$ is a group under function composition and $\text{Aut}_\sigma(G) \leq \text{Sym}_\sigma^+(G) \leq \text{Sym}(G)$. The groups $\text{Sym}_\sigma^-(G)$ and $\text{Sym}_\sigma^+(G)$ are the same by virtue of the following lemma.

Lemma 8. *Let G be an additive group, $\sigma \in \text{Aut}_{\text{Group}}(G)$, and $\tau \in \text{Sym}(G)$. Then the following are equivalent:*

- (a) $\tau(a - \mathcal{O}) = \tau(a) - \tau(\mathcal{O})$ for all $a \in G$ and (σ) -orbits \mathcal{O} of G .
- (b) $\tau(a + \mathcal{O}) = \tau(a) + \tau(\mathcal{O})$ for all $a \in G$ and (σ) -orbits \mathcal{O} of G .

PROOF: If either part (a) or (b) holds then $\tau(0) = 0$. To see this take $a = 0$ and $\mathcal{O} = \{0\}$, where 0 is the neutral element of G . Let \mathcal{O} be a (σ) -orbit of G . Then $-\mathcal{O}$ is an orbit also since σ is a homomorphism.

Suppose part (a) holds. Then $\tau(-\mathcal{O}) = -\tau(\mathcal{O})$ as $\tau(-\mathcal{O}) = \tau(0 - \mathcal{O}) = \tau(0) - \tau(\mathcal{O}) = -\tau(\mathcal{O})$. Hence $\tau(a + \mathcal{O}) = \tau(a - (-\mathcal{O})) = \tau(a) - \tau(-\mathcal{O}) = \tau(a) - (-\tau(\mathcal{O})) = \tau(a) + \tau(\mathcal{O})$ for all $a \in G$. We have shown part (a) implies part (b).

Suppose part (b) holds. Let $a \in \mathcal{O}$. Then $0 = \tau(0) \in \tau(a - \mathcal{O}) = \tau(a) + \tau(-\mathcal{O})$ which means $-\tau(a) \in \tau(-\mathcal{O})$. Therefore $-\tau(\mathcal{O}) \subseteq \tau(-\mathcal{O})$. As a result $\tau(-\mathcal{O}) = -(-\tau(-\mathcal{O})) \subseteq -\tau(-(-\mathcal{O})) = -\tau(\mathcal{O})$. We have shown $\tau(-\mathcal{O}) = -\tau(\mathcal{O})$ and consequently part (a) follows from part (b). \square

Since $\text{Sym}_\sigma^-(G)$ and $\text{Sym}_\sigma^+(G)$ are the same group we use the notation $\text{Sym}_\sigma(G)$ to represent it. To highlight the relationships:

$$\text{Sym}_\sigma(G) := \text{Sym}_\sigma^-(G) = \text{Sym}_\sigma^+(G).$$

In the last section we constructed examples with $\text{Aut}_\sigma(G) < \text{Sym}_\sigma^-(G)$. In this section we construct examples where $\text{Aut}_\sigma(G) < \text{Sym}_\sigma(G)$ of a very different sort; these have three (σ) -orbit lengths instead of two. In the next section we will give sufficient conditions for $\text{Aut}_\sigma(G) = \text{Sym}_\sigma(G)$.

Let X be a set and $A, B \subseteq X$. Recall that $A \setminus B = \{a \in A \mid a \notin B\}$. When $B = \{b\}$ we write $A \setminus b$ for $A \setminus \{b\}$. Now suppose $f : X \rightarrow Y$ is a map of sets. Then $f(A) \setminus f(B) \subseteq f(A \setminus B)$ and

$$(12.2) \quad f(A \setminus B) = f(A) \setminus f(B) \text{ when } f \text{ is one-one.}$$

We will use this fact several times in the construction of our examples.

Let R be a finite commutative local ring with maximal ideal $\mathcal{M} = Rm$, where $m^2 = 0 \neq m$. The set of units of R is $R^\times = R \setminus \mathcal{M}$. Since $R = R^\times \cup \mathcal{M}$ it follows that $\mathcal{M} = R^\times m \cup \{0\}$. Let $a \in R$. Then $L_a : R \rightarrow R$ defined by $L_a(x) = a + x$ for all $x \in R$ belongs to the group $\text{Sym}(R)$ of permutations of R under function composition. Thus $L_a(R^\times) = L_a(R \setminus \mathcal{M}) = L_a(R) \setminus L_a(\mathcal{M})$, or

$$(12.3) \quad a + R^\times = R \setminus (a + \mathcal{M}),$$

for all $a \in R$ by (12.2). As a consequence

$$(12.4) \quad a + R^\times = R^\times$$

for all $a \in \mathcal{M}$.

Let $\mathcal{O}_0 = \{0\}$, $\mathcal{O}_1 = R^\times$, and $\mathcal{O}_2 = R^\times m$. Then $R = \mathcal{O}_0 \cup \mathcal{O}_1 \cup \mathcal{O}_2$ and $\mathcal{O}_i \cap \mathcal{O}_j = \emptyset$ unless $i = j$. Now suppose $\tau \in \text{Sym}(G)$ satisfies $\tau(\mathcal{O}_i) = \mathcal{O}_i$ for $0 \leq i \leq 2$ and the restriction $\tau|_{\mathcal{O}_1} = \text{Id}_{\mathcal{O}_1}$. For such a τ we have:

Lemma 9. $\tau(a + \mathcal{O}_i) = \tau(a) + \tau(\mathcal{O}_i)$ for all $a \in R$ and $0 \leq i \leq 2$.

PROOF: Let $a \in R$. Then $a \in \mathcal{O}_j$ for some $0 \leq j \leq 2$. Since $\mathcal{O}_0 = \{0\}$, $\tau(0) = 0$ and $\tau(a + \mathcal{O}_i) = \tau(a) + \tau(\mathcal{O}_i)$ when $j = 0$ or $i = 0$. Thus we may assume $1 \leq i, j \leq 2$.

Case 1: $i = 1$.

We must show $\tau(a + R^\times) = \tau(a) + \tau(R^\times)$, that is $\tau(a + R^\times) = \tau(a) + R^\times$, for $a \in R^\times$ or $a \in R^\times m$. Since τ is one-one $\tau(a + R^\times) = R \setminus \tau(a + \mathcal{M})$ by (12.2) and (12.3).

Suppose $a \in R^\times$. By assumption $\tau|_{\mathcal{O}_1} = \text{Id}_{\mathcal{O}_1}$. Therefore $\tau(a) = a$; also $\tau(a + \mathcal{M}) = a + \mathcal{M}$ by (12.4). As a consequence

$$\tau(a + R^\times) = R \setminus \tau(a + \mathcal{M}) = R \setminus (a + \mathcal{M}) = a + R^\times = \tau(a) + \tau(R^\times)$$

since $\tau(R^\times) = R^\times$.

Suppose $a \in R^\times m$. Then $a, \tau(a) \in \mathcal{M}$ which means $a + R^\times = R^\times = \tau(a) + R^\times$ by (12.4). Hence $\tau(a + R^\times) = \tau(a) + \tau(R^\times)$.

Case 2: $i = 2$.

We must show that $\tau(a + R^\times m) = \tau(a) + \tau(R^\times m)$, that is $\tau(a + R^\times m) = \tau(a) + R^\times m$, for $a \in R^\times$ or $a \in R^\times m$. First of all assume that $a \in R^\times$. Since $a + R^\times m \subseteq R^\times$ by (12.4), and $\tau|_{\mathcal{O}_1} = \text{Id}_{\mathcal{O}_1}$ by assumption, $\tau(a + R^\times m) = a + R^\times m = \tau(a) + R^\times m$.

Now suppose $a \in R^\times m$. Since $R^\times m = \mathcal{M} \setminus 0$ and $a \in \mathcal{M}$, by (12.2) we have $a + R^\times m = L_a(\mathcal{M}) \setminus L_a(0) = \mathcal{M} \setminus a$. Therefore $a + R^\times m = \mathcal{M} \setminus a$. As a result $\tau(a) + R^\times m = \mathcal{M} \setminus \tau(a) = \tau(a + R^\times m)$; the first equation follows from the preceding equation since $\tau(a) \in R^\times m$ and the second follows from the same by (12.2). Our proof of the lemma is complete. \square

We next show that

$$(12.5) \quad |\mathcal{O}_1| > |\mathcal{O}_2| \geq |\mathcal{O}_0|,$$

which boils down to $|\mathcal{O}_1| > |\mathcal{O}_2|$, or $|R^\times| > |R^\times m|$. Now $|R^\times| \geq |R^\times m|$. Suppose $|R^\times| = |R^\times m|$ and set $r = |R^\times m|$. Then $|\mathcal{M}| = r + 1$ and $|R| = |R^\times| + |\mathcal{M}| = 2r + 1$. Since \mathcal{M} is a proper additive subgroup of R , $\ell|\mathcal{M}| = |R|$ for some $\ell \geq 2$. But then $\ell(r + 1) = 2r + 1$ which is not possible. We have established (12.5).

Now assume R^\times is cyclic with generator u . Then $\sigma \in \text{Aut}_{\text{Group}}(R^+)$, where R^+ denotes the underlying additive group of R and σ is defined by $\sigma(a) = ua$ for all $a \in R$. For $a \in R$ let $\mathcal{O}_{\sigma,a}$ denote the (σ) -orbit of G generated by a . The (σ) -orbits of R are $\mathcal{O}_{\sigma,1} = R^\times = \mathcal{O}_1$, $\mathcal{O}_{\sigma,m} = R^\times m = \mathcal{O}_2$ and $\mathcal{O}_{\sigma,0} = \{0\} = \mathcal{O}_0$. Let $\tau \in \text{Sym}_\sigma(R^+)$. Since $\sigma \circ \tau = \tau \circ \sigma$ the (σ) -orbits of R are permuted by τ . As $\tau(0) = 0$, in light of (12.5) we see $\tau(\mathcal{O}_i) = \mathcal{O}_i$ for $0 \leq i \leq 2$. Also $\tau(ua) = u\tau(a)$ for all $a \in R$ since σ and τ commute; thus $\tau(u^\ell a) = u^\ell \tau(a)$ for all $\ell \in \mathbb{Z}$ and $a \in R$.

(12.6) If $\tau \in \text{Aut}_\sigma(R^+)$ and $\tau(1) = 1$ then $\tau = \text{Id}_R$.

PROOF: Assume the hypothesis of (12.6). Since $\tau(u^\ell) = u^\ell \tau(1) = u^\ell$ for all $\ell \in \mathbb{Z}$ and R^\times is generated by u , $\tau(a) = a$ for all $a \in R^\times$. Let $a \in \mathcal{M}$. Then $1+a \in R^\times$ by (12.4). Therefore $1+a = \tau(1+a) = \tau(1) + \tau(a) = 1 + \tau(a)$ from which $\tau(a) = a$ follows. Since $R = R^\times \cup \mathcal{M}$ we have established (12.6). \square

(12.7) $\text{Aut}_\sigma(R^+) = (\sigma)$.

PROOF: First of all $(\sigma) \subseteq \text{Aut}_\sigma(R^+)$ since $\sigma \in \text{Aut}_\sigma(R^+)$. Conversely, let $\tau \in \text{Aut}_\sigma(R^+)$. Then $\tau(1) \in \tau(\mathcal{O}_1) = R^\times$ which means $\tau(1) = u^s$ for some $s \in \mathbb{Z}$ since u generates R^\times . Since $\sigma^s(1) = u^s$ also, $\sigma^{-s} \circ \tau(1) = 1$, and therefore $\sigma^{-s} \circ \tau = \text{Id}_R$ by (12.6). We have shown that $\tau = \sigma^s \in (\sigma)$. Consequently $\text{Aut}_\sigma(R^+) \subseteq (\sigma)$. \square

Let $r = |R^\times m|$. Then $|\mathcal{M}| = r + 1$. For $s \in \mathbb{Z}$ define $\tau_s \in \text{Sym}(R)$ by $\tau_s(a) = a$ for $a \in R^\times \cup \{0\}$ and $\tau_s(a) = \sigma^s(a)$ for $a \in R^\times m$. Then $\tau_s \circ \sigma = \sigma \circ \tau_s$, $\tau_s(\mathcal{O}_i) = \mathcal{O}_i$ for $0 \leq i \leq 2$, and $\tau_s|_{\mathcal{O}_1} = \text{Id}_{\mathcal{O}_1}$. Using Lemma 9 we conclude that $\tau_s \in \text{Sym}_\sigma(R^+)$. Since $\tau_0 = \text{Id}_R$ and $\tau_s \circ \tau_{s'} = \tau_{s+s'}$ for $s, s' \in \mathbb{Z}$ it follows that $G_2 = \{\tau_s \mid s \in \mathbb{Z}\}$ is a subgroup of $\text{Sym}_\sigma(R^+)$. Noting that $r = |R^\times m| = |\mathcal{O}_{\sigma,m}|$ it is an easy exercise to show that the map $\mathbb{Z}_r \rightarrow G_2$ given by $s \mapsto \tau_s$ is an isomorphism of groups and that $G_2 = \{\tau \in \text{Sym}_\sigma(R^+) \mid \tau|_{R^\times} = \text{Id}_{R^\times}\}$.

Proposition 6. *Let R be a finite commutative local ring with maximal ideal $\mathcal{M} = Rm$, where $m^2 = 0 \neq m$. Suppose that R^\times is cyclic with generator u and let $\sigma \in \text{Aut}_{\text{Group}}(R^+)$ be defined by $\sigma(a) = ua$ for all $a \in R$. Then*

$$\text{Sym}_\sigma(R^+) \simeq \text{Aut}_\sigma(R^+) \times G_2 \simeq \mathbb{Z}_s \times \mathbb{Z}_r,$$

where $s = |R^\times|$ and $r = |\mathcal{M}| - 1$.

PROOF: Let $\tau \in \text{Aut}_\sigma(R^+)$ and $\tau' \in G_2$. Then $\tau \circ \tau' \in \text{Sym}_\sigma(R^+)$ so $f : \text{Aut}_\sigma(R^+) \times G_2 \rightarrow \text{Sym}_\sigma(R^+)$ given by $f((\tau, \tau')) = \tau \circ \tau'$ is well-defined. Now $\tau = \sigma^s$ for some $s \in \mathbb{Z}$ by (12.7). Therefore $\tau \circ \tau' = \tau' \circ \tau$

which implies that f is a group homomorphism. We will show that f is an isomorphism.

Suppose $\tau \circ \tau' = \text{Id}_R$. Then $1 = \tau(\tau'(1)) = \tau(1)$ which implies $\tau = \text{Id}_R$ by (12.6). Therefore $\tau' = \text{Id}_R$ as well. We have shown that f is one-one.

To show that f is onto let $\tau'' \in \text{Sym}_\sigma(R^+)$. Then $\tau''(u^\ell) = u^\ell \tau''(1)$ for all $\ell \in \mathbb{Z}$. Now $\tau''(1) = u^s$ for some $s \in \mathbb{Z}$. Since $\sigma^s(u^\ell) = u^{s+\ell} = \tau''(1)u^\ell = \tau''(u^\ell)$ for all $\ell \in \mathbb{Z}$ we have that $(\sigma^{-s} \circ \tau'')|_{R^\times} = \text{Id}_{R^\times}$. Therefore $\sigma^{-s} \circ \tau'' \in G_2$ and $f((\sigma^s, \sigma^{-s} \circ \tau'')) = \tau''$. We have shown that f is onto. Thus f is an isomorphism. The second isomorphism of the theorem follows from the first and the facts that $|\langle \sigma \rangle| = |R^\times|$, (12.7), and $\mathbb{Z}_r \simeq G_2$; the latter was noted above. \square

Corollary 11. *Let p be a positive prime and $G = \mathbb{Z}_{p^2}$ or $G = \mathbb{Z}_p \oplus \mathbb{Z}_p$. Then there exists a $\sigma \in \text{Aut}_{\text{Group}}(G)$ such that $\text{Aut}_\sigma(G) \simeq \mathbb{Z}_{p(p-1)}$ and $\text{Sym}_\sigma(G) \simeq \mathbb{Z}_{p(p-1)} \times \mathbb{Z}_{(p-1)}$. Hence $\text{Aut}_\sigma(G) < \text{Sym}_\sigma(G)$ when $p > 2$.*

PROOF: The ring \mathbb{Z}_{p^2} has p^2 elements, is local, and has maximal ideal \mathcal{M} with p elements generated by p . The units of \mathbb{Z}_{p^2} are easily seen to form a cyclic group. For odd primes and all $n \geq 1$ the units of \mathbb{Z}_{p^n} form a cyclic group [2, Theorem 26]. The hypothesis of Proposition 6 is satisfied with $R = \mathbb{Z}_{p^2}$.

Let $F = \mathbb{Z}_p$ be the field with p elements and consider the polynomial algebra $F[x]$. The quotient of $R = F[x]/(x^2)$ has p^2 elements, is a local ring, and identifying cosets with representatives has basis $\{1, x\}$. Its maximal ideal $\mathcal{M} = Fx$ has p elements and $x^2 = 0 \neq x$. In particular $|R^\times| = p(p-1)$; indeed $R^\times = \{a + bx \mid a, b \in F, a \neq 0\}$. Since F is a finite field F^\times is cyclic. Let v be a generator of F^\times . Then v has order $p-1$. Observe that $1+x$ is a unit of R order p . Therefore $u = v(1+x)$ is a unit of R order $(p-1)p$ and consequently generates R^\times . Thus R satisfies the hypothesis of Proposition 6. As a vector space $R = F \oplus F$ which means $R = \mathbb{Z}_p \oplus \mathbb{Z}_p$ as an abelian group. \square

13. SUFFICIENT CONDITIONS FOR $\text{Aut}_\sigma(G) = \text{Sym}_\sigma(G)$

Note that $\text{Aut}_\sigma(G) = \text{Sym}_\sigma(G)$ when $\sigma = \text{Id}_G$. We consider involutions.

Theorem 12. *Suppose that G is a finite abelian group of odd order and $\sigma \in \text{Aut}_{\text{Group}}(G)$ has order two. Then $\text{Aut}_\sigma(G) = \text{Sym}_\sigma(G)$.*

PROOF: Let $\tau \in \text{Sym}_\sigma(G)$. We need only show that τ is an endomorphism of G . Now let $a, b \in G$. Then $\tau(a + \mathcal{O}_{\sigma,b}) = \tau(a) + \tau(\mathcal{O}_{\sigma,b})$. Therefore if $\mathcal{O}_{\sigma,b}$ is a singleton set $\tau(a + b) = \tau(a) + \tau(b)$. Since G is abelian the preceding equation holds if $\mathcal{O}_{\sigma,a}$ is a singleton set.

Suppose $\tau(a + b) \neq \tau(a) + \tau(b)$. Then neither $\mathcal{O}_{\sigma,a}$ nor $\mathcal{O}_{\sigma,b}$ are singleton sets and therefore each has two elements since $\sigma^2 = \text{Id}_G$. From the equation $\tau(a + \mathcal{O}_{\sigma,b}) = \tau(a) + \tau(\mathcal{O}_{\sigma,b})$ we deduce the first two of four equations, namely: $\tau(a + b) = \tau(a) + \tau(\sigma(b))$ and $\tau(a + \sigma(b)) = \tau(a) + \tau(b)$. Since G

is commutative, with the roles of a and b reversed, these equations can be written $\tau(a + b) = \tau(\sigma(a)) + \tau(b)$ and $\tau(\sigma(a) + b) = \tau(a) + \tau(b)$. Using the first and third we deduce

$$\tau(\sigma(a + b)) = \sigma(\tau(a + b)) = \sigma(\tau(a) + \tau(\sigma(b))) = \tau(\sigma(a)) + \tau(b) = \tau(a + b).$$

Since τ is one-one $\sigma(a + b) = a + b$; therefore $a + b$ is a fixed point of σ . Using the second and fourth equations we deduce that $a + \sigma(b)$ is a fixed point of σ . Therefore $2a + b + \sigma(b)$ is a fixed point. Consequently $2a$ is a fixed point of σ since $b + \sigma(b)$ is.

By assumption $(2m + 1)a = 0$ for some $m \geq 0$. Since $2a$ is a fixed point of σ so is $-a = m(2a)$ and therefore $\sigma(a) = a$. But this means $\mathcal{O}_{\sigma,a} = \{a\}$, a contradiction. We have shown that $\tau(a + b) = \tau(a) + \tau(b)$ after all. \square

We next show in many cases the question of whether $\text{Aut}_\sigma(G) = \text{Sym}_\sigma(G)$ reduces to the case when σ has one fixed point. Suppose that G is a finite abelian group and $\sigma \in \text{Aut}_{\text{Group}}(G)$. Let G_σ be the subgroup of fixed points of σ and set $\overline{G} = G/G_\sigma$. Let $\overline{\sigma} \in \text{Aut}_{\text{Group}}(\overline{G})$ be defined by $\overline{\sigma}(a + G_\sigma) = \sigma(a) + G_\sigma$ for all $a \in G$.

Let $\tau \in \text{Sym}_\sigma(G)$. Since τ permutes the (σ) -orbits of G it permutes the fixed points of σ . Hence $\tau(G_\sigma) = G_\sigma$. We have noted $\tau(a + b) = \tau(a) + \tau(b)$ whenever a or b generates a singleton (σ) -orbit, that is whenever a or b is a fixed point of σ . Therefore $\overline{\tau} : \overline{G} \rightarrow \overline{G}$ given by $\overline{\tau}(a + G_\sigma) = \tau(a) + G_\sigma$ for all $a \in G$ is well-defined. It is easy to see that $\overline{\tau} \in \text{Sym}_{\overline{\sigma}}(\overline{G})$.

Theorem 13. *Suppose G is a finite abelian group and $\sigma \in \text{Aut}_{\text{Group}}(G)$. Let $\overline{G} = G/G_\sigma$ and suppose that the order of σ and $|G|$ are relatively prime.*

- (a) $\overline{\sigma}$ has one fixed point in \overline{G} .
- (b) Let $\tau \in \text{Sym}_\sigma(G)$. If $\overline{\tau} \in \text{Aut}_{\overline{\sigma}}(\overline{G})$ then $\tau \in \text{Aut}_\sigma(G)$.

PROOF: We first show part (a). Suppose $a \in G$ and $\overline{\sigma}(a + G_\sigma) = a + G_\sigma$. Then $\sigma(a) - a \in G_\sigma$. Set $f = \sigma(a) - a$. Then $\sigma(a) = a + f$. Consequently a and $a + f$ generate $\mathcal{O}_{\sigma,a}$. Let $|\mathcal{O}_{\sigma,a}| = r$. Expressing the sum of the elements of $\mathcal{O}_{\sigma,a}$ in two ways gives $\sum_{\ell=0}^{r-1} \sigma^\ell(a) = \sum_{\ell=0}^{r-1} \sigma^\ell(a + f) = \sum_{\ell=0}^{r-1} \sigma^\ell(a) + rf$ which means $rf = 0$. Since r divides the order of σ it follows that r and $|G|$ are relatively prime. Therefore $f = 0$ which means $\sigma(a) = a$. Thus $a \in G_\sigma$ which means $a + G_\sigma = G_\sigma$. Part (a) is established.

Assume the hypothesis of part (b). Let $a, b \in G$. Writing $\overline{x} = x + G_\sigma$ for $x \in G$ we have $\overline{\tau}(\overline{a} + \overline{b}) = \overline{\tau}(\overline{a}) + \overline{\tau}(\overline{b})$, or $\tau(a + b) - \tau(a) - \tau(b) \in G_\sigma$. Let $f \in G_\sigma$ be this difference. Thus $\tau(a + b) - \tau(a) = \tau(b) + f$. Now $\tau(a + b) = \tau(a) + \tau(\sigma^i(b))$ for some $0 \leq i < r$, where $r = |\mathcal{O}_{\sigma,b}|$. The two equations preceding the last imply $\tau(\sigma^i(b)) = \tau(b) + f$. Since $\tau(\sigma^i(b)) = \sigma^i(\tau(b))$ both $\tau(b)$ and $\tau(b) + f$ generate the same (σ) -orbit. In the proof of part (a) we established $f = 0$; hence $\tau(a + b) = \tau(a) + \tau(b)$. We have shown that $\tau \in \text{Aut}_\sigma(G)$. \square

REFERENCES

- [1] Abe, E. (1980). *Hopf algebras* (translated from the Japanese by Hisae Kinoshita and Hiroko Tanaka), Cambridge Tracts in Mathematics **74**, Cambridge University Press, Cambridge-New York, xii+284 pp.
- [2] Dickson, L. E. (1957). *Introduction to the Theory of Numbers*. Dover Publications, Inc., New York, viii+183 pp.
- [3] Dăscălescu, S., Năstăsescu, C. and Raianu, S. (2001). *Hopf algebras, An introduction*, Monographs and Textbooks in Pure and Applied Mathematics, **235**. Marcel Dekker, Inc., New York, x+401 pp.
- [4] Dummit, D. S. and Foote, R. M. (1999). *Abstract Algebra*, Prentice Hall, New York, xiv+898 pp.
- [5] Lambe, L. A. and Radford, D. E. (1997). *Introduction to the quantum Yang-Baxter equation and quantum groups: an algebraic approach*, Mathematics and its Applications **423**. Kluwer Academic Publishers, Dordrecht, xx+293 pp.
- [6] Majid, S. (1993). Braided matrix structure of the Sklyanin algebra and of the quantum Lorentz group, *Comm. Math. Phys.* **156**, pp. 607-638.
- [7] Majid, S. (1994). Algebras and Hopf algebras in braided categories, in *Advances in Hopf algebras* (Chicago, IL, 1992), Lecture Notes in Pure and Appl. Math. 158, Dekker, New York, pp. 55-105.
- [8] Montgomery, S. (1993). *Hopf algebras and their actions on rings*, CBMS Regional Conference Series in Mathematics **82**. Published for the Conference Board of the Mathematical Sciences, Washington, DC, by the American Mathematical Society, Providence, RI, xiv+238 pp.
- [9] Radford, D. E. (1985). Biproducts and Kashina's Examples, *Comm. Alg.*, to appear.
- [10] Radford, D. E. (2012). *Hopf algebras*, Series on Knots and Everything, **49**. World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2012. xxii+559 pp.
- [11] Radford, D. E. (1985). The structure of Hopf algebras with a projection, *J. Algebra* **92**, pp. 322-347.
- [12] Radford, D. E. and Towber, J. (1993). Yetter-Drinfel'd categories associated to an arbitrary bialgebra, *J. Pure Appl. Algebra* **87**, pp. 259-279.
- [13] Rotman, J. J. (2002). *Advanced modern algebra*, Prentice Hall, Inc., Upper Saddle River, NJ, xvi+1012+A8+B6+I14 pp.
- [14] Sweedler, M. E. (1969) *Hopf algebras*, Mathematics Lecture Notes Series W. A. Benjamin, Inc., New York, vii+336 pp.
- [15] Yetter, D. N. (1990). Quantum groups and representations of monoidal categories, *Math. Proc. Cambridge Philos. Soc.* **108**, pp. 261-290.

UNIVERSITY OF ILLINOIS AT CHICAGO, DEPARTMENT OF MATHEMATICS, STATISTICS AND, COMPUTER SCIENCE (M/C 240), 801 SOUTH MORGAN STREET, CHICAGO, IL 60608-7045

E-mail address: radford@uic.edu